

Gathering Electronic Evidence

from Online Services Providers
in Administrative Punitive
Proceedings

EDITED BY
Stanisław TOSZA
and
Salomé LANNIER

University of Luxembourg

Gathering Electronic Evidence

from Online Services Providers
in Administrative Punitive
Proceedings

EDITED BY
Stanisław TOSZA
and
Salomé LANNIER



**Co-funded by
the European Union**



This project was funded by the European Commission / the Directorate-General for European Anti-Fraud Office under the EUAF-2022-TRAI. Name of the action: ‘Gathering electronic evidence for administrative investigations – comparative study of law and practice - ELEVADMIN’.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Directorate-General for European Anti-Fraud Office. Neither the European Union nor the granting authority can be held responsible for them.

University of Luxembourg

© the authors 2025

This publication is protected by international copyright law.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher.

ISBN 978 2 87996 144 6

ISBN 978-2-87996-144-6



9 782879 961446

TABLE OF CONTENTS

List of authors.....	V
List of abbreviations and acronyms	XV

1. SHEDDING LIGHT: ELECTRONIC EVIDENCE IN ADMINISTRATIVE INVESTIGATIONS	1

S. Tosza, S. Lannier and M. Siclari

2. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN THE EU	13

M. Siclari and S. Tosza

3. GATHERING OF ELECTRONIC EVIDENCE FOR THE PROTECTION OF THE FINANCIAL INTERESTS OF THE EU	63

M. Siclari and J. A. E. Vervaele

4. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN BELGIUM.....	87

V. Franssen and M. Vandormael

5. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN FINLAND.....	131

J. Riekkinen

6. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN FRANCE.....	175

M. Lassalle

7. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN GERMANY	207

P. Blume, M. Gahn, J. Reichmann, C. Zoller, and D. Brodowski

8. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN IRELAND.....	251

N. Ni Loideain

9. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN ITALY	273
<i>G. Lasagni</i>	
10. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN LUXEMBOURG.....	301
<i>S. Lannier and S. Tosza</i>	
11. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN THE NETHERLANDS	341
<i>A. de Vries, L. Mustert, M. Luchtman, A. Duijkersloot, and R. Widdershoven</i>	
12. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN POLAND.....	385
<i>K. Kaszubowski and S. Steinborn</i>	
13. GATHERING ELECTRONIC EVIDENCE IN ADMINISTRATIVE PROCEEDINGS: COMPARATIVE ANALYSIS OF LAW AND PRACTICE.....	405
<i>S. Tosza, S. Lannier and F. Jung</i>	
14. POLICY RECOMMENDATIONS	451
<i>S. Tosza and S. Lannier</i>	
 Annex I Questionnaire for national rapporteurs.....	 462
Detailed table of contents	471

LIST OF AUTHORS

Stanisław Tosza is Associate Professor in Compliance and Law Enforcement at the University of Luxembourg, where he teaches and researches comparative and European criminal law, white-collar crime, compliance law and cyberlaw. He is also the co-Director of the Bachelor in Law programme. Before joining the University of Luxembourg, he was assistant professor at the Willem Pompe Institute of Criminal Law and Criminology at Utrecht University and previously a postdoctoral researcher at the University of Liège. As visiting researcher, he spent also time at Georgetown University Law Center, D.C. (2019), Berkman Klein Center at Harvard University (2017) and Max Planck Institute for Foreign and International Criminal Law in Freiburg i.B. (2008-2010). He defended cum laude his PhD thesis on criminal liability of managers for excessive risk-taking at Utrecht University and at the University of Luxembourg in 2016. Besides numerous articles, he published the monography ‘Criminal Liability of Managers in Europe. Punishing Excessive Risk White Collar Crime’ (Hart 2018), and three collective volumes: ‘White collar crime. A Comparative Perspective’ (Hart 2018), ‘Combatting illicit trade in tobacco products’ (Springer 2022) and ‘The Cambridge Handbook of Digital Evidence in Criminal Investigations’ (Cambridge University Press 2025). Since 2019, he has been the Secretary General of the International Association of Penal Law (AIDP).

Salomé Lannier is a Post-Doctoral Researcher at the University of Luxembourg. Her expertise mainly lies in the fight against human trafficking, a gender-based approach to law, and the legal framework around sex work. She is the PI of project ‘PROtect against EXploitation: exploitative offences versus legitimate work in a digitalised labour market’. Before PROTEX, Salomé was working on the ELEVADMIN project, and on two interdisciplinary projects within the FutureFinTech National Centre of Excellence in Research (NCER), on automatised data protection and anti-money laundering compliance. Salomé is a doctor of law and criminal sciences, after defending in 2023 her thesis on ‘New technologies and human trafficking’, in joint supervision between the University of Bordeaux (France) and the University of Valencia (Spain).

Philipp Blume is an Academic Research Associate and PhD Candidate at the Chair for Europeanisation, Internationalisation and Digital Transformation of Criminal Law and Criminal Procedure of Prof. Dominik Brodowski. His main research topic is modern approaches to telecommunications surveillance.

Dominik Brodowski is a Professor of Europeanisation, Internationalisation and Digital Transformation of Criminal Law and Criminal Procedure at Saarland University, Saarbrücken, Germany, and its Cluster of European Research (CEUS), and he serves as the university's Vice-President for Internationalisation and European Relations. He obtained a Dr. iur. from the University of Tübingen and a LL.M. from the University of Pennsylvania. He focuses on European Criminal Law, Criminal Justice and the Digital Transformation, Constitutional Criminal Justice, and the Foundations and Frontiers of Criminal Justice.

Ton Duijkersloot is an Assistant Professor of Administrative Law at Utrecht University, and a member of the Utrecht Centre for Regulation and Enforcement in Europe (RENFORCE) and the Utrecht Centre for Accountability and Liability Law (UCALL). His research focuses on the interaction between EU law and national administrative law in the areas of law enforcement, administrative justice, general principles of law, fundamental rights and state liability. He has been involved in various courses in bachelor and master study programs, coordinates, *inter alia*, the Research and Thesis Trajectory in the master Constitutional and Administrative Law and has contributed to various research projects and has published many studies about the beforementioned topics, *inter alia*, together with Rob Widdershoven the chapter Administrative law enforcement of EU law in the *Research Handbook on the Enforcement of EU Law* (Edward Elgar 2023).

Vanessa Franssen is Professor at the University of Liège (Belgium) and Co-director of the *Service de droit pénal, de procédure pénale et de droit pénal international*. Furthermore, she is affiliated Senior Researcher at the Institute of Criminal Law of the KU Leuven, where she obtained her PhD in 2013. Until February 2024, she also was a member of the Brussels bar. Previously, she was a Fulbright Fellow at the University of Michigan Law School (USA, 2011-2012) and a post-doctoral researcher at the University of Luxembourg (2014-2015). She studied Law and Romance Languages at the KU Leuven and at the Panthéon-Sorbonne University of Paris 1. She specialises in cybercrime, EU criminal law, economic and financial criminal law, national and comparative criminal law and criminal procedure. She has specific experience in comparative and interdisciplinary research (e.g. data

protection law). She is particularly interested in the impact of new technologies (including artificial intelligence) on criminal law and criminal procedure. Another prong of her research focuses on the interplay between criminal and quasi-criminal enforcement questioning, among other things, the objectives and effectiveness of different enforcement mechanisms. She is the author of numerous publications and conference papers. She has published several collective volumes, including punitive administrative or ‘quasi-criminal’ enforcement (Franssen and Harding, *Criminal and Quasi-criminal Enforcement Mechanisms in Europe. Origins, Concepts, Future*, Hart, 2022), and on the impact of new technologies on criminal law (Franssen and Flore, *Société numérique et droit pénal. Belgique, France, Europe*, Larcier/Bruylant, 2019). Together with Prof. Stanislaw Tosza (University of Luxembourg), she is co-editor of the *Cambridge Handbook on Digital Evidence in Criminal Matters* (Cambridge University Press, 2025). Furthermore, she is an associate editor of the *European Law Blog* (<http://europeanlawblog.eu/>), a widely read academic blog on EU law, and the co-editor of the *International Encyclopaedia of Laws – Criminal Law* (Kluwer Law International), a book series on criminal law and criminal procedure. Finally, she is consulted regularly by European and national policymakers on, for instance, e-evidence, data retention, the data protection regime applicable to the European Public Prosecutor’s Office and the future of EU criminal justice.

Maria Gahn is an Academic Research Associate and PhD Candidate at the Chair for Europeanisation, Internationalisation and Digital Transformation of Criminal Law and Criminal Procedure of Prof. Dominik Brodowski. Her main research topics are cybercrime, data protection and victimology.

Flora Jung is a Research and Development Specialist in Criminal Law at the University of Luxembourg. Before joining the University of Luxembourg, she completed an internship at the Court of Justice of the European Union and worked as a Research Assistant at PluriCourts – Centre for the Study of the Legitimate Roles of the Judiciary in the Global Order, a Norwegian Centre of Excellence at the University of Oslo. She holds an LL.M. in Public International Law, with a specialisation in Peace, Security, and International Law, from the University of Oslo, and a bachelor’s degree in law from the University of Luxembourg.

Krzysztof Kaszubowski is an Adjunct Professor at the Department of Administrative Proceedings, Faculty of Law and Administration, University of Gdańsk. He served as a member of the Local Government Appeals Board in Gdańsk from 2001 to 2023, and as its Vice-President from 2009 to 2015.

Since 2023, he has been serving as a judge at the Voivodship Administrative Court in Gdańsk. He is the author of several dozen publications, specialising in administrative proceedings, enforcement proceedings, and administrative court proceedings.

Giulia Lasagni is a Senior Assistant Professor at the University of Bologna. She has a Ph.D. in Criminal Procedure Law, was a post-doctoral researcher at the University of Luxembourg and a Visiting Researcher at the University of North Carolina, Wrocław and Paris-Nanterre. She has worked in the legal department of the Single Supervisory Mechanism (SSM) of the European Central Bank and at the European Anti-Fraud Office (OLAF). Her main research topics include: the application of algorithmic and AI technologies to the criminal justice matter; procedural safeguards in criminal proceedings in Italy and in the case law of the European Courts; miscarriages of justice; new forms of digital investigations and surveillance; banking and financial investigation; and information flows in AML/CFT investigations. She is part of several national and European research projects, both as principal investigator and as researcher (among which FACILEX, ParTFin, CROSSJUSTICE, ECB Legal Research Programme, DEVICES, EUBAR) and the author of several papers, as well as of the monograph ‘Banking Supervision and Criminal Investigation. Comparing the EU and US Experiences’ (Springer/Giappichelli, 2019).

Maxime Lassalle is an Associate Professor at the University of Burgundy (France), where he teaches and conducts research in banking law, criminal law, white-collar crime, compliance law, and data protection. Before joining the University of Burgundy in 2021, he was a post-doctoral researcher at the Max Planck Institute for the Study of Crime, Security and Law. Prior to that, he completed his PhD at the University of Luxembourg and at the Paris Nanterre University. In 2019, he defended his PhD thesis on transnational access to bank data. As a visiting researcher, he has been affiliated with the University of Illinois (2016), George Washington University (2017), and the University of Ottawa (2025). He is the author of a monograph published by Larcier in 2021 and co-editor, alongside Dr. Benjamin Vogel and Prof. Eleni Kosta, of the collective volume ‘Law of Public-Private Cooperation against Financial Crime’ (Intersentia, 2024).

Michiel Luchtman is a Professor of Economic and European criminal law. He chairs the Willem Pompe Institute for Criminal Law and Criminology. He is also one of the programme leaders of the Utrecht Centre for Regulation and Enforcement in Europe (RENFORCE) and of the master European criminal justice in a global context. His research and teaching focus

on the consequences of Europeanisation for criminal justice and law enforcement in general; on criminal law and fundamental rights; on economic criminal law, as well as criminal tax law. He also (co-)supervises several PhD projects on these issues. He is the Dutch contact point of ECLAN, the EU criminal law academic network. From September 2019 until September 2022, he was the director of masters education and board member of the Utrecht Law School.

Lisette Mustert is an Assistant Professor of Administrative Law at Utrecht University, and a member of the Utrecht Centre for Regulation and Enforcement in Europe (RENFORCE). She conducts research at the intersection of EU and national administrative law. Her expertise lies particularly in the field of supervision and enforcement in the EU, composite administrative decision-making procedures, and the protection of fundamental rights such as the right to an effective judicial remedy. Her research interests also include questions of effectiveness and good administration in the supervision of the General Data Protection Regulation and enforcement of EU laws more generally. She has written several journal articles and book chapters and presented her research findings at (international) conferences and seminars. Prior to joining Utrecht University, she defended her doctoral thesis on ‘Cross-border enforcement of the GDPR by independent administrative authorities’ at the University of Luxembourg, under the supervision of Professor Herwig Hofmann.

Nora Ni Loideain is Senior Lecturer in Law and Director of the Information Law & Policy Centre at the Institute of Advanced Legal Studies, University of London. Her research concerns EU law and European human rights law, particularly privacy and data protection in the areas of law enforcement and national security. In 2019, she was appointed to the UK Home Office Biometrics and Forensics Ethics Group which provides independent advice on biometrics governance for public security. She is Editor-in-Chief of *International Data Privacy Law* (Oxford University Press). In 2024, she was co-author on an AI and biometrics regulation report for the Alan Turing Institute and was an expert witness to the House of Lords on UK-EU data adequacy. Her book on privacy rights, data retention law, and mass surveillance in the EU and ECHR legal orders is the first doctrinal and comparative analysis of these standards within the contexts of serious crime and national security: Ni Loideain, ‘EU Data Privacy Law and Serious Crime’ (OUP 2025). Previously, she was a Policy Officer for the Office of the Director of Public Prosecutions of Ireland and clerked for the Irish Supreme

Court. She holds BA, LLB, LLM degrees (National University of Ireland, Galway) and a PhD in law (University of Cambridge).

Julia Reichmann is an Academic Research Associate and PhD Candidate at the Chair for Europeanisation, Internationalisation and Digital Transformation of Criminal Law and Criminal Procedure of Prof. Dominik Brodowski. Their main research topic is anti-money laundering instruments on a European level.

Juhana Riekkinen is a University Lecturer in Legal Informatics at the University of Lapland, Faculty of Law. His monograph dissertation, which was accepted with honours and published commercially in 2019, combined evidence law with perspectives from the field of legal informatics, examining the life-cycle of digital data within the context of the Finnish legal framework on the gathering, presentation, and evaluation of evidence in criminal proceedings. In addition, he has authored or co-authored over 30 publications, including 13 peer-reviewed articles or chapters in edited volumes, on a wide range of issues pertaining to the relationships between information, ICT, and law. Specifically, his expertise covers themes such as investigatory powers, exclusion of evidence, online fraud, the burden of explanation in criminal cases, freedom of expression and platform regulation, data protection, and regulation of artificial intelligence. He has previously worked on projects focusing on blockchain technology (Powered by Blockchain, funded by the European Social Fund) and predictive AI applications in the field of healthcare and social services (MAITE, funded by the Finnish Ministry of Social Affairs and Health). He is currently responsible for the teaching of legal informatics at the Faculty of Law. Furthermore, he possesses experience in teaching procedural law and frequently lectures at training events for judges, lawyers, prosecutors, and other professionals. In addition to his academic career, he has completed training at the bench at the District Court of Lapland and the Court of Appeal of Rovaniemi.

Martina Siclari was a Research and Development Specialist in Criminal Law at the University of Luxembourg. Prior to joining the University of Luxembourg, she worked as intern at the Court of Justice of the European Union and within the Legal Service of the European Public Prosecutor's Office (EPPO). She holds a Master's degree in Law from the University of Bologna, Italy and an LL.M. in EU Law from the Institute for European Studies of the Université libre de Bruxelles (IEE-ULB). As of 2025, Martina also serves as Legal Assistant in the Legal Service of the EPPO.

Slawomir Steinborn is a Professor of Criminal Procedure and European Criminal Law at the University of Gdańsk (Poland), and head of the Department of Criminal Procedure Law and Criminalistics at the Faculty of Law and Administration. He conducted research at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany: from April 2008 to June 2009 as a fellow of the Alexander von Humboldt Foundation, and in August 2015 as a fellow of the Max Planck Society. Since 2016, he has served as a judge at the Court of Appeal in Gdańsk, where he was appointed President in March 2025 for a six-year term. In April 2024, he was nominated by the Prime Minister to the Commission for the Codification of Criminal Law under the Polish Ministry of Justice (he previously served on this Commission from 2013 to 2016). He is the author or co-author of over 150 scientific publications in Polish, German, and English, as well as more than 20 expert reports prepared for the Polish Parliament, the Ministry of Justice, the Ministry of Foreign Affairs, and the Council of Europe. He has participated in numerous domestic and European research projects. He is a member of the Polish group of AIDP, a member of the AIDP Scientific Committee (elected in June 2025), and a member of the European Criminal Policy Initiative. He also serves as President of the Polish Humboldt-Fellow club, *Societas Humboldtiana Polonorum* (2023–2026). His research interests include criminal law and procedure, international cooperation in criminal matters, European criminal law (particularly the harmonisation of criminal law and procedure, and judicial cooperation), as well as the criminal aspects of constitutional law.

Mathilde Vandormael is a Teaching and Research Assistant at the *Service de droit pénal, de procédure pénale et de droit pénal international* of the University of Liège (Belgium). Her research primarily explores business criminal law in all its dimensions, with a particular focus on the intersection between criminal law and punitive administrative law. Beyond academia, she is an active member of the Brussels Bar, where she advises and represents clients in criminal and punitive administrative investigations, trials, and alternative dispute resolution procedures. Her expertise in business criminal law benefits from a dual perspective, having practiced both as a defense lawyer and within an enforcement authority. She holds degrees in both business management and law, equipping her with a comprehensive understanding of the complexities inherent to business criminal law. She has consistently deepened her specialisation in this field and is the founder of the Belgium Chapter of the Women in White Collar Defense Association.

John A. E. Vervaele became emeritus professor at Utrecht Law School in 2023. He was elected president of the International Association of Criminal Law (AIDP) from 2014 to 2024, of which he became honorary president. He is a member of the Member of the Steering Committee of ECLAN, the European Criminal Law Academic Network, Brussels. He has been teaching at the College of Europe since 1996. His main areas of teaching are criminal law and criminal procedure, economic and financial criminal law, European criminal justice, enforcement of Union law, EU law and human rights, comparative criminal justice, terrorism and criminal procedure. He has realised a lot of research in these areas, both for Dutch Departments and European Institutions and worked as well as a consultant for them. He has been very active in the field of European criminal law both in the area of enforcement of community law and in Area of Freedom, Security and Justice. Beside his scholarly work, he had the lead of several research projects in the field, both for Dutch Ministries and the European Community and the European Union. M. Delmas Marty and he directed the Corpus Juris project 2000. He was also strongly involved in the establishment of the European Public Prosecutor's Office (EPPO). He is regularly teaching as visiting professor in foreign universities, in Europe and overseas (United States of America, Latin America, China), mostly topics touching upon economic and financial criminal law, European criminal law, international criminal law and judicial cooperation in criminal matters. His teaching is not limited to the University but does include regularly teaching to the judiciary.

Aart de Vries is an Assistant Professor of (European) criminal law at the Willem Pompe Institute and the Utrecht Centre for Regulation and Enforcement in Europe (RENFORCE). In 2024, he obtained his PhD cum laude for his dissertation *Evidence and Transnational Punitive Enforcement Proceedings in the European Union* (Eleven Publishing 2024). In his dissertation, he studies the gathering, sharing, and use of evidence in cross-border criminal and punitive-administrative proceedings in the EU. Starting from a comparative law analysis of the implementation of EU enforcement obligations in the fields of customs, transfrontier waste shipment, and market abuse in the Netherlands, Germany, and France, he determines whether and, if so, in what way differences between the enforcement architecture in the Member States and the national and European law rules and standards on the gathering, sharing, and use of evidence in cross-border cases create problems for effective enforcement on the one hand, and the protection of fundamental rights on the other. His research focuses primarily on the interface between national and EU criminal and administrative (procedural) law, and the interface between criminal and administrative law enforcement, also from a European perspective. Various topics enjoy his special interest, such as

judicial cooperation in criminal matters between EU Member States, cross-border use of (unlawfully obtained) evidence, the role of fundamental rights and the EU Charter, including effective legal protection in cross-border cases, and the European Public Prosecutor's Office (EPPO). He gives lectures and seminars in various LLM and bachelor courses. He also supervises students writing their theses in the Utrecht School of Law's bachelor programme, the master programme in Dutch Criminal Law and the English-language master programme in European Criminal Justice in a Global Context. Since July 2023, he has also been the coordinator of the latter LLM. Besides his PhD thesis, he has made several academic contributions (articles, chapters in edited volumes, presentations at conferences) in English and Dutch and is (or has been) involved in several major research projects.

Rob Widdershoven is a Professor of European Administrative Law at Utrecht University. His research focuses on the interaction between EU law and national administrative law in the areas of law enforcement, administrative justice, general principles of law, fundamental rights and state liability. Moreover, he increasingly studies questions of composite and transnational decision-making and enforcement. About these topics he published about 250 articles, books and reports. He received several prizes, amongst them the main publication prize of the Dutch Association of Administrative Law, which he was awarded twice. He is member of the Board of Editors of the *Review of European Administrative Law* (REALaw) and of several Dutch journals, amongst them *Overheid & Aansprakelijkheid* (Government & Liability) and *JBplus* (Journal of Administrative Case Law). Since 2013, he is Advocate General of Administrative Law in the Netherlands. In this function, he is member of the Dutch Council of State, the Trade and Industry Appeals Court and the Central Appeals Court.

Christoph Zoller is an Academic Research Associate and PhD Candidate at the Chair for Europeanisation, Internationalisation and Digital Transformation of Criminal Law and Criminal Procedure of Prof. Dominik Brodowski. His main research topic is cybercrime investigations.

LIST OF ABBREVIATIONS AND ACRONYMS

ABoR	Administrative Board of Review
ABRvS	Dutch Administrative Jurisdiction Division of the Council of State, <i>Afdeling bestuursrechtspraak van de Raad van State</i>
ACD	Luxembourgish Direct Taxes Administration, <i>Administration des Contributions Directes</i>
ACM	Dutch Authority for Consumers and Markets, <i>Autoriteit Consument en Markt</i>
ACPR	French Prudential Control and Resolution Authority, <i>Autorité de Contrôle Prudentiel et de Résolution</i>
ADA	Luxembourgish Customs and Excise Administration, <i>Administration des Douanes et des Accises</i>
ADM	Italian Customs and Monopolies Agency, <i>Agenzia delle Dogane e dei Monopoli</i>
AEDT	Luxembourgish Registration, Domains and VAT Administration, <i>Administration de l'enregistrement, des domaines et de la TVA</i>
AFM	Dutch Authority for the Financial Markets, <i>Autoriteit Financiële Markten</i>
AFP	Australian Federal Police
AGCM	Italian Competition Authority, <i>Autorità Garante della Concorrenza e del Mercato</i>
AMF	French financial market authority, <i>Autorité des Marchés Financiers</i>
ANPR	Automatic Number Plate Recognition
AP	Dutch Data Protection Authority, <i>Autoriteit Persoonsgegevens</i>
ASP	Irish Administrative Sanctions Procedure
BaFin	German Federal Financial Supervisory Authority, <i>Bundesanstalt für Finanzdienstleistungsaufsicht</i>
BCA	Belgian Competition Authority
Benchmark Regulation	Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments

	and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014
BZSt	German Federal Central Tax Office, <i>Bundeszentralamt für Steuern</i>
CAA	Luxembourgish Insurances Commissariat, <i>Commissariat aux Assurances</i>
CAB	Irish Criminal Assets Bureau
CBb	Dutch Trade and Industry Appeals Tribunal, <i>College van Beroep voor het bedrijfsleven</i>
CBI	Central Bank of Ireland
CCP	Code of Criminal Procedure
CCPC	Irish Competition and Consumer Protection Commission
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the EU
CNIL	French data protection authority, <i>Commission Nationale Informatique et Liberté</i>
CNPD	Luxembourgish National Commission for Data Protection, <i>Commission nationale pour la protection des données</i>
ComReg	Irish Commission for Communications Regulation
Consob	Italian Financial Market Supervisory Authority, <i>Commissione Nazionale per le Società e la Borsa</i>
CRAR	Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies
CRD IV and V	Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC
CREG	Commission for Electricity and Gas Regulation
CRR I and II	Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012

CRvB	Dutch Central Appeals Tribunal, <i>Centrale Raad van Beroep</i>
CSSF	Luxembourgish Financial Sector Supervisory Commission, <i>Commission de Surveillance du Secteur Financier</i>
DAC7	Council Directive (EU) 2021/514 of 22 March 2021 amending Directive 2011/16/EU on administrative cooperation in the field of taxation
DG COMP	Directorate-General for Competition of the European Commission
DPA	Data Protection Authority
DPC	Irish Data Protection Commissioner
DRG	Irish Digital Regulators Group
EBU	European Banking Union
ECB	European Central Bank
ECHR	European Charter of Human Rights
ECJ	European Court of Justice
ECN	European Competition Network
ECN+	Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market
ECtHR	European Court of Human Rights
EDIS	European Deposit Insurance Scheme
EIO	European Investigation Order
EMIR	Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories
EPPO	European Public Prosecutor's Office
ESMA	European Securities and Markets Authority
EU	European Union
FBI	Federal Bureau of Investigation
FCCA	Finnish Competition and Consumer Authority, <i>Kilpailu ja kuluttajavirasto</i>
FCCA	Finnish Competition and Consumer Authority
FIN-FSA	Financial Supervisory Authority, <i>Finanssivalvonta</i>
FIN-FSA	Finnish Financial Supervisory Authority
FIOD	Dutch Fiscal Information and Investigation Service, <i>Fiscale Inlichtingen- en Opsporingsdienst</i>

FIU	Financial Intelligence Unit
FRA	European Union Agency for Fundamental Rights
FSC	Polish Financial Supervision Commission, <i>Komisja Nadzoru Finansowego</i>
FSMA	Financial Services and Markets Authority
FTC	US Federal Trade Commission
GACE	General Administration of Customs and Excise
GDF	Italian military economic police, <i>Guardia di Finanza</i>
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
GPDP	Italian Data Protection Authority, <i>Garante per la protezione dei dati personali</i>
DTA	General Tax Administration
HADOPI	French administration in charge of intellectual property, <i>Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet</i>
IBPT	Belgian Institute for Postal Services and Telecommunications
IFSAT	Irish Financial Appeals Tribunal
IIO	Independent Investigating Officer
IOSCO	International Organisation of Securities Commissions
ISPs	Internet Service Providers
LPP	Legal Professional Privilege
MAR, Market Abuse Regulation	Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC
Markkinaoikeus	Finnish Market Court
MICAR	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No

	1095/2010 and Directives 2013/36/EU and (EU) 2019/1937
MIFID II	Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU
MiFIR	Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012
MMS	Multimedia Messaging Service
MoU	Memoranda of Understanding
NBB	National Bank of Belgium
NCAs	National Competent Authorities
OCCP	Polish Office of Competition and Consumer Protection, <i>Prezes Urzędu Ochrony Konkurencji i Konsumentów</i>
OLAF	European Anti-Fraud Office
OSPs	Online Services Providers
PDPO	Polish Personal Data Protection Office, <i>Prezes Urzędu Ochrony Danych Osobowych</i>
PIN	Personal Identification Numbers
PRIIPS	Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investment products
PUK	Personal Unlocking Keys
SIS	Special Inspection Service
SMS	Short Media Service
SRM	Single Resolution Mechanism
SSM	Single Supervisory Mechanism
TFEU	Treaty on the Functioning of the European Union
The Controller	Controller of Procedural guarantees
Tietosuoja-valtuutettu	Finnish Data Protection Ombudsman
Traficom	Finnish Transport and Communications Agency
Tulli	Finnish Customs
UCC	Union Customs Code (Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code)
UCITS Directive	Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in

	financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU
VAT	Value Added Tax
Verohallinto	Finnish Tax Administration
VREG	Flemish Regulator of the Electricity and Gas Market
WRC	Irish Workplace Relations Commission

1. SHEDDING LIGHT: ELECTRONIC EVIDENCE IN ADMINISTRATIVE INVESTIGATIONS

S. TOSZA, S. LANNIER and M. SICLARI

1. INTRODUCTION

With the ever-increasing digitalisation of almost every aspect of human activities any type of infringement – be it criminal or administrative – leaves digital traces, which may be crucial as evidence in punitive proceedings. According to a study by the European Commission, around 85% of criminal investigations require electronic evidence to be obtained.¹ The peculiarity of electronic evidence – contrary to more traditional sources of evidence – lies in its potential to be obtained through a third party, most notably the service provider holding the data. This feature is unique. By way of illustration, although access to physical correspondence was, already in the past, possible as an investigation measure, traditional postal services did not retain access to the content of the communications they delivered, nor did they regularly gather metadata associated with those letters. To the contrary, email service providers normally do both. While the possibility to acquire data from telecommunication providers appeared earlier, in recent years it is the access to data from Online Service Providers (OSPs) that has become crucial for successful investigations.

Likewise, the rapid evolution of technology continues to reshape the behaviour and methods of perpetrators of fraud and irregularities affecting the EU budget. Too often, such irregularities hide behind perfect paper presentations. Artificial circumstances created to unlawfully obtain EU funding through practices such as collusion, under-valuation or other wrongdoing, can only be effectively detected and revealed through access to information held by OSPs. To name just few examples, investigations

¹ European Commission, *Impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, Commission staff working document, SWD/2018/118 final, UE, 17/04/2018, p. 14.

increasingly rely on the availability of evidence sourced from social media platforms, while fraudsters seem to increasingly (ab)use the deep and dark web to facilitate illicit financial transactions, particularly involving cryptocurrencies. Ongoing studies into the application of blockchain technology in the context of EU funding and public procurement highlights the pressing need for legal framework to adapt to the evolving technological landscape.²

Although access to electronic evidence for the purpose of criminal investigation has been subject to extensive research efforts, there has been no systematic research to date in the field of administrative investigations as to the legal possibilities for requesting electronic evidence from OSPs. There has been no knowledge about the practice itself, in particular as regards the use of a general legal basis or voluntary cooperation. These matters are the subject of the project ‘Gathering electronic evidence for administrative investigations – comparative study of law and practice’ – ELEVADMIN, co-financed by the Union Anti-fraud Programme (EUAf), of which this book is the outcome.³

2. ELECTRONIC EVIDENCE: FROM CRIMINAL TO PUNITIVE ADMINISTRATIVE PROCEEDINGS

2.1. Towards the E-evidence Regulation

Data that is in possession of OSPs may be a treasure trove for law enforcement authorities. However, accessing OSPs’ data is hindered by the clash of the nature of cyberspace and the limitations of enforcement. While data flows unhindered – at least in certain countries – law enforcement is confined to the national borders as prescribed in the seminal *Lotus* judgment.⁴ The principle of territoriality mandates, in its conventional reading, that if the data is stored outside of the country of investigation, then instruments of cross-border cooperation need to be used, which renders the access much more time-consuming, costly, and cumbersome. This duality – attractiveness

² European Commission, ‘European Blockchain Pre-Commercial Procurement’, 02/10/2021, online <https://digital-strategy.ec.europa.eu/en/news/european-blockchain-pre-commercial-procurement>.

³ The preliminary reflection on the design of this research was published in *Eucrim* 2/2023: S. Tosza, ‘Gathering Electronic Evidence for Administrative Investigations: Exploring an Under-the-Radar Area’, *Eucrim*, 2023, no. 2, pp. 216-222, online <https://eucrim.eu/articles/gathering-electronic-evidence-for-administrative-investigations/>, DOI:10.30709/eucrim-2023-018. This chapter uses portions of that text.

The editors are very grateful for Flora Jung for her invaluable help in drafting the comparative chapter and finalising the formatting of all chapters.

⁴ Permanent Court of International Justice, *SS Lotus*, 07.09.1927, Series A.-No. 70, pp. 18-19.

of electronic evidence gathered from third parties and inaptness of principles governing enforcement to cyberspace – characterises this field and has triggered a number of legislative and jurisprudential initiatives.

Over the past years, the debate over access to electronic evidence gained prominence as regards access to data for criminal investigations. The laws of criminal procedure allowed the authorities to access this data, while protecting suspects' procedural safeguards. However, when the OSP was located in another country or the data was stored abroad, law enforcement was supposed to resort to instruments of cross-border cooperation, such as the European Investigation Order⁵ (EIO) within the Area of Freedom, Security and Justice, and mutual legal assistance (MLA) outside this area, in particular as regards content data from US companies.⁶

The paperwork of mutual legal assistance (MLA) and the length of the procedure, necessary even in purely local simple cases, garnered frustration of law enforcement and led to the use of voluntary cooperation with OSPs and to a reinterpretation of the principle of territoriality. As to the latter, Belgium for instance decided to treat foreign providers actively targeting Belgian clients in the same way as if they were national providers.⁷ In two famous cases concerning Yahoo and Skype these companies found themselves obliged to produce data according to a Belgian order, while the law of the place where they were headquartered (United States and Luxembourg respectively) forbade them to do so.⁸

Three major initiatives aimed to remedy this situation, although it is too early to assess their impact. The European Union (EU) has recently adopted a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (the E-evidence Regulation),⁹ which aims at addressing the above-mentioned difficulties. Most importantly, it will allow law enforcement authorities in one Member State to compel service providers in another Member State to produce data without engaging the authorities of

⁵ Directive 2014/41/EU of the European Parliament and of the Council of 03.04.2014 regarding the European Investigation Order in criminal matters.

⁶ J. Daskal, 'Unpacking the CLOUD Act', *Eucrim*, 2018, no. 4, pp. 220-225, online <https://eucrim.eu/articles/unpacking-cloud-act/>, DOI:10.30709/eucrim-2018-022.

⁷ V. Franssen, 'The Belgian Internet Investigatory Powers Act - A Model to Pursue at European Level Reports: Practitioner's Corner', *European Data Protection Law Review*, 2017, vol. 3, no. 4, pp. 534-542.

⁸ P.D. Hert, M. Kopcheva, 'International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case', *Computer Law & Security Review*, 2011, vol. 27, no. 3, pp. 291-297.

⁹ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12.07.2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings.

the latter.¹⁰ This Regulation is also linked with the potential agreement with the United States, which would broaden the possibilities of US OSPs to produce data to foreign law enforcement.¹¹ Finally, the recently adopted Second Protocol to the Cybercrime Convention¹² also provides for possibilities of directly requesting data cross-border, even if it would apply only to limited types of data.

2.2. The gap around administrative law enforcement

Notably absent from these debates and initiatives is administrative law enforcement.¹³ Yet, electronic evidence is no less crucial for both national and European punitive administrative proceedings. While, due to fundamental rights concerns, the access to electronic evidence will arguably not be as broad as for criminal investigations, it will be increasingly more difficult to miss the golden opportunity that access to evidence through OSPs offers for effective investigations, including within the administrative domain. Even non-content data can provide valuable insights, which may prove essential to

¹⁰ V. Franssen, S. Tosza (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Matters*, Cambridge, United Kingdom, Cambridge University Press, 2025; S. Tosza, 'Mutual recognition by private actors in criminal justice? E-evidence regulation and service providers as the new guardians of fundamental rights', *Common Market Law Review*, 2024, vol. 61, no. 1, DOI:10.54648/cola2024005; S. Tosza, 'European Union · The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?', *European Data Protection Law Review*, 2023, vol. 9, no. 2, pp. 163-172, DOI:10.21552/edpl/2023/2/11; S. Tosza, 'Internet service providers as law enforcers and adjudicators. A public role of private actors', *Computer Law & Security Review*, 2021, vol. 43, p. 105614, DOI:10.1016/j.clsr.2021.105614; S. Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order', *New Journal of European Criminal Law*, 2020, vol. 11, no. 2, pp. 161-183, DOI:10.1177/2032284420919802; S. Tosza, 'Cross-border gathering of electronic evidence: mutual legal assistance, its shortcomings and remedies', in: V. Franssen, D. Flore, F. Stasiak (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 269; S. Tosza, 'The European Commission's Proposal on Cross-Border Access to E-Evidence : Overview and Critical Remarks', *Eucrim*, 2018, no. 4, pp. 212-219, online <https://eucrim.eu/articles/european-commissions-proposal-cross-border-access-e-evidence/>, DOI:10.30709/eucrim-2018-021.

¹¹ United States Department of Justice, 'Joint US-EU Statement on Electronic Evidence Sharing Negotiations', 26.09.2019, online <https://www.justice.gov/archives/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations>.

¹² Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

¹³ Tosza, (n. 3). See the exception of S. Mason, U. Rasmussen, *The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof. A comparative study and analysis*, CDCJ(2015)14 final, Strasbourg, European Committee on Legal Co-operation, Council of Europe, 2016.

substantiating evidence of misconduct.¹⁴ So far, no comprehensive research has been done on the powers of administrative punitive authorities to gather electronic evidence from OSPs or about safeguards for affected persons on that context.

2.2.1. Gathering electronic evidence for administrative enforcement authorities

The possibilities of acquiring electronic evidence from third parties (in that case, OSPs) for evidentiary purposes are no less attractive or necessary in administrative proceedings than in criminal investigations. In this regard, we can already distinguish at least three different ways for administrative enforcement authorities to gather such evidence.

Firstly, there may be a concrete legal basis allowing them to make such requests. For instance, the Market Abuse Regulation¹⁵ provides that under certain circumstances competent authorities shall have the power to request existing data traffic records held by a telecommunications operator.¹⁶ However, in particular at the national level, such access may be controversial. For instance, the French legal framework regarding access to telecommunication data by administrative authorities evolved considerably during the last few years. Relying on the case law of the European Court of Justice (ECJ), the Constitutional Council struck down several laws that did not adequately address privacy and data protection considerations.¹⁷ One interesting feature of the current legal framework is the creation of a new authority (*le contrôleur des demandes de données de connexion*) in charge of allowing these measures in some administrative sectors.¹⁸

Secondly, data may be potentially requested from OSPs by means of a more general legal basis of requests for information. For instance, at the EU level, the European Central Bank (ECB) may request data based on Article 10(1)(f) of the SSM Regulation no. 1024/2013.¹⁹ Likewise, Directorate-General for Competition of the European Commission (DG COMP) may request information from third parties based on Article 18 of Regulation

¹⁴ B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company, 2016.

¹⁵ Regulation (EU) no. 596/2014 of the European Parliament and of the Council of 16.04.2014 on market abuse (Market Abuse Regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.

¹⁶ Article 23 (2) (h) Market Abuse Regulation.

¹⁷ Conseil Constitutionnel, 25.02.2022, no. 2021-976/977 QPC.

¹⁸ Article L. 621-10-2 Code monétaire et financier.

¹⁹ Council Regulation (EU) no. 1024/2013 of 15.10.2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions.

1/2003,²⁰ which does not preclude using it to request information from OSPs. Similarly, competent national authorities may proceed in a comparable manner, relying on general legal bases within their domestic legal framework.

Thirdly, administrative enforcement authorities may simply request data from service providers on a voluntary basis. Such a practice has emerged particularly in the context of criminal investigations, as a pragmatic response to the shortcomings of coercive mechanisms for obtaining such data, as outlined above. It relies on the general willingness of OSPs to cooperate with law enforcement and allows the authorities to avoid the problem of territoriality and the necessity to use cooperation instruments. At the same time, these requests are not binding for OSPs. Furthermore, OSPs may tend to check fundamental rights compliance of requests, which creates distorted dynamics between public and private authorities, with potentially detrimental results for persons concerned or interests of investigations at stake.²¹

A very particular case in that context is offered by OLAF: a body, with an objective to conduct investigations of misconduct, the results of which should transform into national criminal proceedings. The relevance of electronic evidence for those investigations is no less evident than for criminal proceedings. Yet, OLAF at this point does not seem to have the power to directly request such data from OSPs, which might be essential for detection or investigation of irregularities affecting the Union budget.

2.2.2. Regulating investigations in a world of interconnected law enforcement authorities

The need for electronic evidence arises in the punitive landscape in which the boundary between administrative and criminal enforcement within both national and European legal systems has become progressively blurred, especially in complex areas such as taxation and financial compliance. This raises important questions regarding the legal safeguards applicable to investigative powers, particularly in light of existing data protection standards.²² As administrative authorities increasingly engage in fact-finding activities that mirror criminal investigations in both scope and intrusiveness, ensuring the appropriate calibration of procedural guarantees has become a critical issue for the legitimacy and accountability of hybrid enforcement regimes.

²⁰ Council Regulation (EC) no. 1/2003 of 16.12.2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.

²¹ Tosza, 'Internet service providers as law enforcers and adjudicators', (n. 10).

²² K. Ligeti, S. Tosza, 'Challenges and Trends in Enforcing Economic and Financial Crime: Criminal Law and Alternatives in Europe and the US', in: K. Ligeti, S. Tosza (eds.), *White collar crime: a comparative perspective*, Oxford, Hart publishing, Hart studies in European criminal law vol. 7, 2019, pp. 1-34.

In the contemporary legal landscape, where national and supranational law enforcement authorities increasingly operate in a coordinated manner, the regulation of investigative procedures must adapt to a reality characterised by legal hybridity and institutional interdependence. Irregularities may fall within the realm of either administrative or criminal law, and thus the choice of investigative framework may reveal strategic.

Administrative proceedings are generally perceived as more flexible, with fewer procedural constraints and lower thresholds for initiating inquiries. However, whenever new evidence emerges, such proceedings – initially framed as administrative – may be requalified as criminal, thereby triggering the application of enhanced procedural safeguards, in line with Article 6 of the European Convention on Human Rights (ECHR).

This fluidity between procedural frameworks is further illustrated by the transfer and mutual admissibility of evidence across domains, a phenomenon sometimes referred to as ‘*vases communicants*’.²³ For instance, electronic evidence gathered in an administrative context may be reused in a parallel or subsequent criminal proceeding, provided that the applicable legal framework allows such transfer. This interconnection is particularly visible in the operational relationship between OLAF and the EPPO. While OLAF conducts administrative investigations into fraud affecting the financial interests of the European Union, its findings – including electronic evidence – may be transmitted to the EPPO to support criminal prosecution. In turn, EPPO may rely on OLAF’s investigative outputs to launch or complement criminal investigations under its competence. This institutional synergy, while promoting efficiency and coherence, also raises important questions regarding procedural guarantees, the scope of admissible evidence, and the potential risk of circumventing criminal procedural safeguards through administrative corridors.²⁴

²³ S. Lannier, ‘Obtention par l’ACD de données auprès d’opérateurs ou de fournisseurs de services de télécommunication. Une étude à la lumière du règlement sur les preuves électroniques en matière pénale’, *Cahiers de fiscalité luxembourgeoise et européenne*, 2024, vol. 2024/2, pp. 23-50. This dynamic was thematised already in the seminal study on the penal provisions for the protection of European finances: M. Delmas-Marty, J. Vervaele (eds.), *The Implementation of the Corpus Juris in the Member States: Penal Provisions for the Protection of European Finances*, Antwerpen, Intersentia, 2000, vols. 1-4.

²⁴ S. Allegrezza, I. Rodopoulos, ‘Interactions Between Administrative and Criminal Law in the Context of the Enforcement of Bank Prudential Regulations’, *Oxford Business Law Blog*, 2016, online <https://blogs.law.ox.ac.uk/business-law-blog/blog/2016/06/interactions-between-administrative-and-criminal-law-context>.

2.3. Perspective from the Council of Europe and the European Court of Human Rights

Administrative authorities often impose sanctions that, while formally labelled as non-criminal, may produce punitive consequences comparable to those of criminal penalties. The European Court of Human Rights (ECtHR) has consistently held that where administrative penalties have a punitive and deterrent effect, they may fall within the scope of Article 6 of the ECHR, thereby triggering the application of criminal procedural guarantees.²⁵

In its seminal judgment *Engel and Others v. The Netherlands*²⁶, the ECtHR established a set of criteria – commonly referred to as the *Engel* criteria – for determining whether a given procedure, although formally administrative, should be regarded as ‘criminal’ in nature for the purpose of the Convention. These include: (1) the legal classification of the offence under domestic law, (2) the nature of the offence, and (3) the severity of the penalty. The Court has emphasised that the latter two carry greater weight in determining the autonomous meaning of ‘criminal charge’ under the Convention. In assessing this, the Court has taken into account a range of factors, including: the general applicability of the legal rule, whether the procedure is initiated by a public authority exercising statutory enforcement powers, whether the rule pursues a punitive or deterrent objective, whether the rule aims to protect general societal interests in a manner comparable to criminal law, whether the imposition of a sanction depends on a finding of guilt, and the classification of similar procedures in other member states of the Council of Europe.

This jurisprudence has had far-reaching implications, particularly in areas of hybrid enforcement where administrative proceedings may entail punitive elements, necessitating the application of criminal procedural safeguards to ensure compliance with the ECHR fair trial guarantees. In particular, Article 6 of the ECHR enshrines a number of defence rights and procedural guarantees that must be implemented in the face of criminal charges, including the presumption of innocence and the right to an independent and impartial tribunal established by law.

This jurisprudential framework is particularly relevant in the context of electronic evidence, where the intrusiveness of investigative measures may resemble those of criminal proceedings. As administrative authorities increasingly rely on data held by private actors, the ECtHR’s case law

²⁵ D. Ohana, ‘Regulatory Offenses and Administrative Sanctions: Between Criminal and Administrative Law’, in: M.D. Dubber, T. Hörnle (eds.), *The Oxford Handbook of Criminal Law*, Oxford University Press, 2014.

²⁶ ECtHR, *Engel and Others v. the Netherlands*, 08.06.1976, nos. 48272/17, 57479/17, 510/18, 7936/18, 27115/18.

provides a crucial benchmark for assessing the legitimacy and proportionality of such practices, thereby anchoring the book's exploration of electronic evidence within a broader human rights paradigm.

3. METHODOLOGY OF THIS RESEARCH

In view of the above considerations and given the exponential increase of significance of electronic evidence, this research aimed at shedding the light on this under-the-radar problem, which is gathering electronic evidence in administrative investigations. This book presents the outcome of this research, which examined the existing legal framework and practice at the national and EU level, compared it critically and formulated recommendations as to the legal framework of gathering electronic evidence in that context. The research followed tailored-made methodology consisting of examining five legal areas at the EU level and across nine legal systems.

3.1. Selected areas of enforcement

The comparative analysis examined five areas of punitive enforcement, namely customs, Value Added Tax, competition law and General Data Protection Regulation (GDPR) enforcement, as well as punitive enforcement in the area of banking and financial markets. These areas were examined to establish legal possibilities to request electronic evidence from OSPs or to transfer such evidence from another proceeding (criminal or administrative). While PIF was the main targeted area for policy recommendations formulated in the last chapter of this book, the four other areas were chosen for comparison due to their thematic and policy proximity and interaction between criminal and administrative enforcement. At the same time each of them offers a different perspective and a different set of experience and challenges.

As to the domain of financial supervision, it was chosen since the Market Abuse Regulation already provides for a possibility to request records held by a telecommunications operator. While market abuse has a strong EU component, this is less prominent for enforcement in customs. Customs duties represent a traditional own source for the EU budget, with 75% of the customs duties collected by EU Member States going to the EU budget.²⁷ The revenue from customs duties is estimated to be about 10% of the total revenues of the EU budget.²⁸

²⁷ Council Decision (EU, Euratom) 2020/2053 of 14.12.2020 on the system of own resources of the European Union and repealing Decision 2014/335/EU, Euratom.

²⁸ G. D'Angelo, *Aspects of customs control in selected EU Member States*, Bologna University Press, 2023.

As to competition law, the enforcement of EU competition law plays a crucial role in maintaining fair market conditions, preventing anti-competitive practices and safeguarding consumer interests. As markets become more integrated and globalised, the complexity of enforcing competition rules has increased, particularly with regard to cross-border mergers, cartels and other anti-competitive agreements, with a prominent role played by DG Competition at the EU level. Finally, as data processing and digitalisation continue to accelerate, ensuring compliance with GDPR has become increasingly complex. The regulation mandates strict controls on data collection, storage, and processing, with severe penalties for non-compliance. The enforcement of GDPR thus requires effective collaboration between national data protection authorities, particularly for cross-border data flows.

While all areas were given equal attention in the research, they shed light on OLAF's investigatory powers, resulting in policy recommendations as to the possibilities for OLAF to extend its powers to gather electronic evidence from OSPs and the parameters for such powers. Furthermore, the study explored to what extent access to information held by OSPs complies with or should be accompanied by supplementary judicial control. The research explored to what extent a system analogous to OLAF's access to bank accounts could be set-up. Within OLAF's administrative investigative remit, such power could be equated to those of national investigators, and rely under conditions of national law, possibly including assistance by the national anti-fraud coordination services and/or judicial review.

3.2. A comparative analysis

The analysis of those five areas was performed at EU and national level. At the national level, it has been conducted using a standard questionnaire²⁹ in the following Member States: Belgium, Finland, France, Germany, Italy, Ireland, Luxembourg, the Netherlands, and Poland. In parallel, a similar analysis into the EU law in the same domains was performed.

At the national level, authorities competent in these selected areas were examined, such as national competitions authorities (*Autorité de la concurrence* in France, UOKiK in Poland), financial supervision authorities (e.g., BAFIN in Germany, CSSF in Luxembourg), and custom and tax investigation authorities (e.g. FIOD: Fiscal Information and Investigation Service in the Netherlands or the General Administration of Customs and Excise in Belgium). Some of these authorities perform tasks in criminal and administrative enforcement. The consequences of that feature for gathering electronic evidence were also examined. Similar investigations were

²⁹ See Annex I at the end of this book.

undertaken at the EU level concerning powers of relevant authorities, such as DG COMP, the ECB or European Securities and Markets Authority (ESMA).

The information thus gathered was subject to a comprehensive comparative analysis. ELEVADMIN established to what extent punitive administrative authorities are granted powers by legislators to request data from OSPs, to which extent they use those powers, and to what extent they need to look for creative solutions to gather data they need for their enforcement activities. This investigation provides sufficient material to understand patterns and tendencies as well as needs of examined authorities. We also examined the findings from the perspective of the fundamental rights standard of protection of privacy.

3.3. A ‘law in action’ analysis

Another key objective of ELEVADMIN was to understand the practice of gathering electronic evidence from OSPs in the context of administrative investigations. To this end, the project adopted a law in action approach, which contrasts with the traditional ‘law in the books’ methodology. While the latter centres on formal legal provisions, a law in action methodology seeks to understand how legal norms are implemented in practice, with particular attention to enforcement practices, administrative behaviour, and the interaction between legal frameworks and technological realities.³⁰

As a result, an integral and highly important part of that research was the examination of the practice of using the identified legal frameworks, as well as in general of gathering electronic evidence from OSPs. This required conducting interviews with representatives of the relevant authorities, stakeholders from the private sector and practitioners.

4. THE STRUCTURE OF THE BOOK

The structure of this book is designed to provide a comprehensive analysis of the legal possibilities of gathering electronic evidence from OSPs in administrative punitive proceedings, combining theoretical, practical and comparative perspectives. Chapter 2 provides an in-depth analysis of the European Union setting, exploring the current legal framework for gathering electronic evidence from third parties in punitive enforcement proceedings in the selected areas at the EU level, with a particular focus on proceedings conducted by DG COMP, the ECB and ESMA. The third chapter specifically addresses the protection of the financial interests of the EU, detailing existing provisions that enable OLAF to collect data from private actors not involved

³⁰ R. Pound, ‘Law in Books and Law in Action’, *American Law Review*, 1910, vol. 44, no. 1, pp. 12-36.

in the context of both its internal and external investigations, as well as the procedural guarantees and the available remedies in place to safeguard the rights of those involved. Chapters 4 through 11 offer country-specific examinations, analysing the legal frameworks and practices in 9 different Member States: Belgium (Chapter 4), Finland (Chapter 5), France (Chapter 6), Germany (Chapter 7), Ireland (Chapter 8), Italy (Chapter 9), Luxembourg (Chapter 10), the Netherlands (Chapter 11), and Poland (Chapter 12). Notably, each chapter presents an extensive examination of national provisions and practices for each punitive administrative enforcement area. A comprehensive comparative analysis is then provided in Chapter 13, which identifies similarities and differences in legal provisions governing administrative proceedings and investigative powers, particularly with regard to the possibility to gather electronic evidence from OSPs across different jurisdictions. The book concludes with Policy Recommendations (Chapter 14), which result from this research as regards both national and European administrative authorities, with a particular attention to OLAF. They focus on the possibilities of using current legal framework to gather electronic evidence in punitive administrative proceedings and examine the question of extending those powers.

2. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN THE EU

M. SICLARI and S. TOSZA

1. COMPETENT AUTHORITIES IN SELECTED AREAS OF PUNITIVE ADMINISTRATIVE ENFORCEMENT¹

This chapter analyses selected areas of punitive enforcement at the EU level. For certain of these areas, EU-level authorities hold direct enforcement powers under EU law, notably the Directorate-General for Competition of the European Commission (DG COMP), the European Central Bank (ECB) and the European Securities and Markets Authority (ESMA). However, other areas, such as the enforcement of the General Data Protection Regulation (GDPR),² as well as customs and VAT enforcement, lack a centralised EU competent authority. For these areas, the chapter will address specific EU-level acts or provisions to the extent that they regulate the enforcement powers of national competent authorities (NCAs) or facilitate cooperation among them.

1.1. DG COMP

The enforcement of competition law has been governed by EU primary law since the very beginning, dating back to the Treaty of Rome establishing

¹ The authors are grateful to all the professionals who shared their expertise and perspectives in the course of this research. Special thanks are due to Jean-François Bellis, Sébastien Thomas and Dr. Olivier Voordeckers whose generous engagement and thoughtful responses provided particularly valuable insights that informed the development of parts of this chapter. All errors are our own.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88.

the European Economic Community in 1957.³ While the public enforcement of EU competition rules has originally been of a centralised nature, with the European Commission serving as the main enforcer and national competition authorities playing only a limited role, the adoption of Regulation 1/2003⁴ has marked a paradigm shift towards a more decentralised system of enforcement.⁵ As of May 2004, the public enforcement of substantive competition rules is jointly conducted by both the Commission under EU law and by NCAs operating within the procedural framework prescribed in their respective national legislation.⁶ Within the Commission, the enforcement of EU competition rules is the main responsibility of DG COMP. This chapter focuses on the investigations carried out by DG COMP for alleged violations of Article 101⁷ and Article 102⁸ of the Treaty on the Functioning of the European Union (TFEU) under Regulation 1/2003.

The Commission's powers of enforcement are currently set out in Regulation 1/2003, which confers upon DG COMP a blend of investigative, prosecutorial, and decision-making functions, subject solely to review by the Court of Justice of the European Union (ECJ). DG COMP may commence an investigation into alleged suspected infringement of competition rules on its own motion or acting upon a complaint. Moreover, many investigations in cartel cases are often triggered by a leniency application (i.e., self-reporting by undertakings involved in a cartel to benefit from either full or partial immunity from fines).

DG COMP's administrative procedure under Regulation 1/2003 is composed of two distinct stages, namely a preliminary investigation stage and

³ M. Bernatt, L. Zoboli, 'Competition law', p. 398, in: M. Scholten (ed.), *Research Handbook on the Enforcement of EU Law*, p. 565, Cheltenham, United Kingdom, Edward Elgar Publishing, 2023.

⁴ Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 4.1.2003, pp. 1-25.

⁵ A. Jones, B. Sufrin, N. Dunne, *Jones and Sufrin's EU competition law: Text, Cases and Materials*, Oxford, United Kingdom, Oxford University Press, 7th ed., 2019; E. Gippini-Fournier, 'The Modernisation of EU Competition Law: First Experiences with Regulation 1/2003', in: H.F. Koeck and M.M. Karollus (eds), *The Modernisation of European Competition Law – Initial Experiences with Regulation 1/2003*, vol. 2, Nomos, 2008; P. Ibáñez Colomo, *The Shaping of EU Competition Law*, Cambridge, United Kingdom, Cambridge University Press, 2018.

⁶ The rules on the allocation of cases among the Commission and NCAs are contained in Article 13 of Regulation 1/2003.

⁷ Article 101 TFEU prohibits 'agreements between undertakings', 'decisions by associations of undertakings' and 'concerted practices' that may affect trade between Member States and restrict competition within the internal market.

⁸ Article 102 TFEU prohibits any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it insofar as it may affect trade between Member States.

an *inter partes* stage.⁹ The preliminary investigation, which extends until the notification of the statement of objections and during which DG COMP uses the powers of investigation provided for in Regulation 1/2003, is intended to enable the gathering of all relevant information to ascertain the existence of an infringement of competition rules and to adopt an initial position.¹⁰ Conversely, the subsequent adversarial stage covers the period from the notification of the statement of objections until the adoption of the final decision.¹¹

Fines are the main tool for DG COMP for enforcing competition rules. Under Regulation 1/2003, the Commission has the power to impose fines on undertakings and associations of undertakings for substantive and procedural infringements of competition law. The gravity and the duration of the infringement should impact the amount of the fine. In any case, fines should not exceed 1% of total turnover in the preceding business year for procedural infringements,¹² and 10% for substantive infringements.¹³ Additionally, DG COMP may impose period penalty payments not exceeding 5% of the average daily turnover in the preceding business year per day, to compel undertakings to comply with its decisions.¹⁴

Notwithstanding the wording of Article 23(5) of Regulation 1/2003, which explicitly states that fines imposed on undertaking under Articles 101 and 102 TFEU shall not be of a ‘criminal law nature’, the case-law of the European Court of Human Rights (ECtHR) has repeatedly considered that fines imposed for competition infringements may be criminal in substance, according to the so-called Engel criteria.¹⁵ In its seminal judgement in the *A. Menarini Diagnostics S.r.l. v. Italy* case, concerning a fine of 6 million euros imposed by the Italian competition authority, the ECtHR held that, notably because of its severity, the fine imposed amounted to a criminal penalty, and hence the criminal limb of Article 6 of the European Convention of Human

⁹ A. Jones, B. Sufrin, N. Dunne, *Jones & Sufrin's EU Competition Law: Text, Cases, and Materials*, Oxford, United Kingdom, Oxford University Press, 7th ed., 2019.

¹⁰ ECJ, *Meta Platforms Ireland Ltd v. European Commission*, 24.05.2023, T-452/20, § 112; ECJ, *Cementos Portland Valderrivas v. Commission*, 14.03.2014, T-296/11, § 33 and the case-law cited.

¹¹ ECJ, *Prym and Prym Consumer v. Commission*, 03.09.2009, C-534/07 P, § 27; ECJ, *Almamet v. Commission*, 12.12.2012, T-2410/09, § 24.

¹² Article 23(1) Regulation 1/2003.

¹³ Article 23(2) Regulation 1/2003.

¹⁴ Article 24 Regulation 1/2003.

¹⁵ ECtHR, *A. Menarini Diagnostics S.r.l. v. Italy*, 27.09.2011, no. 43509/08, § 42.

Rights (ECHR) was applicable.¹⁶ Subsequent judgements of the ECtHR have endorsed such position.¹⁷

Yet, the ECJ's case-law in this regard has not always been straightforward. Despite the initial reluctance of the ECJ to accept the applicability of Article 6 ECHR to such proceedings, this position has progressively changed over time, going so far as to state that the area is 'at least akin to criminal law'.¹⁸ Moreover, the ECJ has consistently found applicable the *ne bis in idem* principle, as enshrined in Article 50 of the Charter of Fundamental Rights of the European Union (Charter), in the field of competition law.¹⁹ That protection has been considered to apply also to competition fines due to their punitive and deterrent nature and their high degree of severity.²⁰ In light of these considerations, despite their administrative label, the nature of competition proceedings might amount to 'quasi-criminal',²¹ which in turn affects the level of applicable procedural guarantees.

1.2. ECB

As regards the punitive enforcement of banking supervision, as of November 2014, the ECB has acquired direct enforcement powers. The Single Supervisory Mechanism (SSM) is one of the three pillars on which the

¹⁶ P. Szilágyi, 'Human Rights Jurisprudence and the Effectiveness of Competition Law Sanction', pp. 242-256, in: T. Tóth (ed.), *The Cambridge Handbook of Competition Law Sanctions*, Cambridge, United Kingdom, Cambridge University Press, 2022.

¹⁷ ECtHR, *Société Stenuit v. France*, 27.02.1992, no. 11598/85; ECtHR, *Jussila v. Finland*, 23.11.2006, no. 73053/01.

¹⁸ ECJ, Opinion of Advocate General Kokott, *Autorità Garante della Concorrenza e del Mercato v. Ente Tabacchi Italiani – ETI Spa*, 03.07.2007, C-280/06, § 71. See also ECJ, Opinion of Advocate General Léger, *Baustahlgewebe GmbH v. Commission*, 03.02.1998, C-185/95 P, § 31.

¹⁹ See, ECJ, *bpost SA v. Autorité belge de la concurrence*, 22.03.2022, C-117/20 and ECJ, *Bundeswettbewerbsbehörde v. Nordzucker AG, Südzucker AG, Agrana Zucker GmbH*, 22.03.2022, C-151/20 'on duplication of proceeding and penalties of a criminal nature in competition law'. The origins of the case-law on *ne bis in idem* in competition matters derive from the seminal *Wilhelm and Others* judgment.

²⁰ P. Rossi, V. Sansonetti, 'Untangling the Inextricable: The Notion of 'Same Offence' in EU Competition Law', *Concurrences*, 2020, no. 3-2020, online <https://www.concurrences.com/en/review/issues/no-3-2020/articles/untangling-the-inextricable-the-notion-of-same-offence-in-eu-competition-law-95557-en>.

²¹ M. Kärner, 'Interplay between European Union criminal law and administrative sanctions: Constituent elements of transposing punitive administrative sanctions into national law', *New Journal of European Criminal Law*, 2022 vol. 13, no. 1, <https://doi.org/10.1177/20322844221085918>.

European Banking Union (EBU) is built.²² The SSM's role is to ensure respect of prudential requirements imposed on banks by the Capital Requirement Regulation (CRR I and II)²³ and the Capital Requirement Directive (CRD IV and CRD V)²⁴, which together form the so-called 'Single Rulebook'. The EBU includes a highly complex shared enforcement system, in which European and national authorities share supervisory, investigatory and sanctioning powers.²⁵ The SSM Regulation²⁶ entrusts the ECB with the enforcement of the Union's policies as regards prudential supervision of credit institutions, as defined in Article 4(1) of the CRR.²⁷ To that aim, specific banking supervision tasks have been conferred by the SSM Regulation on the ECB. The SSM Regulation provides the ECB with a supervisory toolbox composed of investigatory powers, as well as administrative penalties.

As clarified by the ECJ in the *Landeskreditbank* case, the supervisory competence of the ECB is exclusive with regard to all credit institutions. Yet, in order to allocate enforcement powers between the ECB and the NCAs, the SSM Regulation distinguishes supervised entities based on whether they are

²² The other two pillars consist of a Single Resolution Mechanism (SRM) for the orderly resolution of banks, and a European Deposit Insurance Scheme (EDIS) to ensure a common system for deposit protection. In practice, however, the EDIS has not yet been established.

²³ Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012, as amended by Regulation (EU) 2019/876 of the European Parliament and of the Council of 20 May 2019 amending Regulation (EU) No 575/2013 as regards the leverage ratio, the net stable funding ratio, requirements for own funds and eligible liabilities, counterparty credit risk, market risk, exposures to central counterparties, exposures to collective investment undertakings, large exposures, reporting and disclosure requirements, and Regulation (EU) No 648/2012, OJ L 176, 27.6.2013, pp. 1-337.

²⁴ Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance, OJ L 176, 27.6.2013, p. 338-43 as amended by Directive (EU) 2019/878 of the European Parliament and of the Council of 20 May 2019 amending Directive 2013/36/EU as regards exempted entities, financial holding companies, mixed financial holding companies, remuneration, supervisory measures and powers and capital conservation measures, OJ L 150, 7.6.2019, pp. 253-295.

²⁵ S. Allegranza, I. Rodopoulos, 'Enforcing Prudential Banking Regulations in the Eurozone: A Reading from the Viewpoint of Criminal Law', p. 233-264, in: K. Ligeti, V. Franssen (eds.), *Challenges in the Field of Economic and Financial Crime in Europe and the US*, p. 313, London, United Kingdom, Bloomsbury Publishing, 2017.

²⁶ Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions, OJ L 287, 29.10.2013, p. 63-89.

²⁷ Article 1(1) SSM Regulation.

classified as significant or less significant,²⁸ with the supervision of the latter being exercised by the NCAs on a decentralised basis under the responsibility of the ECB.²⁹

This chapter particularly focuses on proceedings of the ECB in the context of investigations into possible breaches of law which may lead to imposing punitive sanctions. The ECB may conduct investigations either as a part of its ongoing supervision mandate – via a ‘Joint Supervisory Team’ tasked with the day-to-day oversight of each significant supervised entity³⁰ – or in response to suspected infringements of EU law.³¹ In practice, challenges arise in distinguishing supervisory functions from investigative activities with a punitive nature.³² In the latter case, the investigation of the infringement shall be referred to the ‘Investigating Unit’,³³ an internal independent unit constituted by investigators appointed by the ECB from among its own staff. The establishment of the Investigating Unit results from the requirement to separate the investigating and decision-making phase when imposing administrative sanctions.³⁴ The Investigating Unit may exercise the investigatory powers granted to the ECB under the SSM Regulation.³⁵ Once the investigation is concluded and the investigating unit deems a sanction appropriate, it must prepare a draft decision outlining the identified violations and the proposed financial penalties, which is then submitted to the

²⁸ According to Article 2(20) of the SSM Framework Regulation, ‘supervised entity’ are defined as meaning any of the following: (a) a credit institution established in a participating Member State; (b) a financial holding company established in a participating Member State; (c) a mixed financial holding company established in a participating Member State, provided that it fulfils the conditions laid down in point (21)(b); (d) a branch established in a participating Member State by a credit institution which is established in a non-participating Member State.

²⁹ ECJ, *Landeskreditbank Baden-Württemberg – Förderbank v. European Central Bank, European Commission*, 8.05.2019, C-450/17 P.

³⁰ Article 3, SSM Framework Regulation. Each joint supervisory team should be composed of ECB and NCAs members.

³¹ M. Scholten, M. Simonato, ‘EU Report’ in: M. Luchtman, J. Vervaele (eds.), *Investigatory powers and procedural safeguards: Improving OLAF’s legislative framework through a comparison with other EU law enforcement authorities (ECN/ESMA/ECB)*, Report, European Commission, OLAF, 2017.

³² On the distinction between supervisory and investigatory phase see, L. Wissink, *Effective Legal Protection in Banking Supervision*, Zutphen, The Netherlands, Europa Law Publishing, 2021.

³³ Article 123 SSM Framework Regulation.

³⁴ R. D’Ambrosio, ‘Due Process and Safeguards of the Persons Subject to SSM Supervisory and Sanctioning Proceedings’, *Quaderni di Ricerca Giuridica della Consulenza Legale*, 2013, no. 74, pp. 48-49, online https://www.bancaditalia.it/pubblicazioni/quaderni-giuridici/2013-0074/Quaderno-74.pdf?language_id=1.

³⁵ Article 125 SSM Framework Regulation.

Supervisory Board,³⁶ and subsequently forwarded to the Governing Council for adoption.³⁷

As a corollary of its investigatory and supervisory powers, the SSM Regulation empowers, in certain cases, the ECB to impose administrative sanctions on supervised credit institutions. Article 18 grants the ECB a direct sanctioning power (i.e., it can impose penalties on supervised entities directly, without relying on NCAs) for two types of breaches. Where supervised entities, intentionally or negligently, breach directly applicable acts of Union law,³⁸ the ECB may impose pecuniary penalties of up to twice the profits gained or losses avoided as a result of the breach, or up to 10% of the total annual turnover in the preceding business year.³⁹ The penalties applied shall be ‘effective, proportionate and dissuasive’.⁴⁰ Furthermore, the ECB can impose sanctions in case of breaches of ECB decisions or regulations.⁴¹ For other types of infringements, the ECB retains only an indirect sanctioning power, namely the power to require NCAs to open proceedings with a view of imposing appropriate penalties.⁴²

Although not formally classified as criminal, the prevailing view in the literature is the substantially punitive nature of respectively the ‘administrative pecuniary penalties’ of Article 18(1) and ‘fines’ mentioned in Article 18(7).⁴³ This punitive character is further supported by their repressive and deterrent nature, as well as the severity of the penalty.

1.3. ESMA

Finally, the EU competent authority in the field of financial markets is ESMA. The latter has been often referred to as ‘the most powerful of all EU

³⁶ The Supervisory Board is not bound to follow the proposal submitted by the Investigating Unit.

³⁷ F. Allemand, ‘The Sanctioning Power of the ECB: From One to Several Legal Regimes’, in: S. Montaldo, F. Costamagna, A. Miglio (eds.), *EU Law Enforcement. The Evolution of Sanctioning Powers*, Routledge, London, 2021.

³⁸ Breaches of requirements of the CRR, as identified in Article 67(1) CRD IV.

³⁹ Article 18(1) SSM Regulation.

⁴⁰ Article 18(3) SSM Regulation.

⁴¹ Article 18(7) SSM Regulation. In this case, the ECB may impose sanctions in accordance with Regulation (EC) No 2532/98.

⁴² Article 18(5) SSM Regulation.

⁴³ Allegrezza, Rodopoulos, (no. 24); V. Felisatti, ‘Sanctioning Powers of the European Central Bank and the Ne Bis In Idem Principle within the Single Supervisory Mechanism’, *European Criminal Law Review*, 2018, vol. 8(3), no. 2018-01, pp. 378-403, DOI: 10.5771/2193-5505-2018-3-378.

agencies’.⁴⁴ Established in 2010 in the aftermath of the 2008 financial crisis as part of a European System of Financial Supervision, ESMA is the EU’s financial markets regulator and supervisor. ‘ESMA’s mission is to enhance investor protection, promote orderly financial markets and safeguard financial stability.’⁴⁵ While lacking direct sanctioning powers of its own under the Market Abuse Regulation (MAR),⁴⁶ ESMA has direct enforcement powers over some key financial entities to deal with possible infringements of relevant sectorial legislation. Credit Rating Agencies,⁴⁷ Trade Repositories,⁴⁸ Securitisation Repositories,⁴⁹ as well as Data Reporting Service Providers,⁵⁰ Tier 2 Third-Country Central Counterparties,⁵¹ and since 2022, administrators of EU critical benchmarks and third-country administrators recognised in the EU,⁵² fall under ESMA’s direct supervision,

⁴⁴ M. Van Rijsbergen, M. Simoncini, ‘Controlling ESMA’s enforcement powers’, in: M. Scholten, A. Brenninkmeijer (eds.), *Controlling EU Agencies*, Cheltenham, United Kingdom, Edward Elgar, 2020; M. Scholten, ‘EU enforcement agencies’, in: M. Scholten (ed.), *Research Handbook on the Enforcement of EU Law*, Cheltenham, United Kingdom, Edward Elgar, 2023.

⁴⁵ ESMA founding Regulation 1095/2010. ESMA Annual Report 2022, p. 17.

⁴⁶ Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, OJ L 173, 12.6.2014, pp. 1-61.

⁴⁷ Regulation (EU) No 462/2013 of the European Parliament and of the Council of 21 May 2013 amending Regulation (EC) No 1060/2009 on credit rating agencies, OJ L 146, 31.5.2013, pp. 1-33.

⁴⁸ Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, OJ L 201, 27.7.2012, pp. 1-59 (EMIR).

⁴⁹ Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation, and amending Directives 2009/65/EC, 2009/138/EC and 2011/61/EU and Regulations (EC) No 1060/2009 and (EU) No 648/2012, OJ L 347, 28.12.2017, pp. 35-80. Under Article 14 SECR, ESMA is granted the same powers conferred to it in accordance with Articles 61 to 68, 73 and 74 of the EMIR.

⁵⁰ Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012, OJ L 173, 12.6.2014, pp. 84-148 (MiFIR), as amended by the ESAs Review envisages that - starting from 1 January 2022 - ESMA is granted direct responsibilities regarding the authorisation and supervision of DRSPs, except for those that fall under a derogation.

⁵¹ The review of the EMIR Regulation, or EMIR 2.2., enhanced the role of ESMA. ESMA received direct supervisory responsibilities for systemically important third country CCPs. TC-CCPs that qualify as ‘systemically important’ (Tier 2 TC-CCPs) that are required to comply with the relevant EMIR requirements (‘Titles IV and V’ and ‘Article 16’) and are subject to supervision by ESMA, in accordance with the mandate outlined under Articles 25(2b) and 25b of EMIR.

⁵² Currently, the only EU critical benchmark is EURIBOR, administered by the European Money Markets Institute (EMMI).

which includes the investigation of possible infringements and, in appropriate cases, taking enforcement action, including imposing fines. As such, ESMA is the only EU agency with direct enforcement powers *vis-à-vis* private parties.⁵³ Where, as part of their daily monitoring activity, ESMA supervisors find indications of a possible violation of the relevant regulations, the case is referred for further investigation to an independent investigating officer (IIO) appointed within ESMA.⁵⁴ Among the investigative powers of the IIO are the power to request information and documents, the power to summon and interview persons, and to execute on-site inspections. The IIO shall investigate the question whether an infringement was committed and may recommend imposition of measures or administrative fines. Based on the file submitted by the IIO, and after having heard the person subject to the investigation, the Board of Supervisors of ESMA independently decides whether the supervised entity has, intentionally or negligently, committed an infringement of the relevant regulations, and issues a decision to impose fines.⁵⁵

As regards the nature of the enforcement, the ECJ has already considered that some of the administrative sanctions that can be imposed in the area of financial markets appear to have a punitive character, pursuing a punitive purpose and presenting a ‘high degree of severity’.⁵⁶

1.4. Customs enforcement

Substantive customs law is standardised at EU level, but its implementation within Member States remains mainly entrusted to national customs authorities, without a centralised EU customs administration.⁵⁷

⁵³ M. van Rijsbergen, M. Scholten, ‘ESMA Inspecting: The Implications For Judicial Control Under Shared Enforcement’, *European Journal of Risk Regulation*, 2016, vol. 7, no. 3, pp. 569-579, DOI: 10.1017/S1867299X00006085.

⁵⁴ See for instance Article 64(1) EMIR and Article 23e(1) CRAR.

⁵⁵ In 2024, ESMA imposed a €2,197,500 fine on Scope Ratings GmbH for five infringements of the CRAR committed with negligence.

⁵⁶ In that sense see the ECJ case-law with reference to proceedings of the Italian Consob in ECJ, *DB v. Consob*, 2.02.2021, C-481/19, § 43; ECJ, *Di Puma and Zecca*, 20.03.2018, C-596/16 and C-597/16, § 38; ECJ, *Garlsson Real Estate and Others v. Commissione Nazionale per le Società e la Borsa (Consob)*, 20.03.2018, C-537/16, §§ 34 and 35. The ECJ, for its part, reached, in essence, the same conclusion in ECtHR, *Grande Stevens and Others v. Italy*, 4.03.2014, no. 18640/10, § 101. H. Andersson, ‘Fighting insider dealing at all costs?—due process aspects on the EU market abuse regime’, *Capital Markets Law Journal*, 2022, vol. 17, issue 2, pp. 196–211, DOI: <https://doi.org/10.1093/cmlj/kmac001>.

⁵⁷ G. D’Angelo, *Aspects of customs control in selected EU Member States*, Bologna, Italy, Bologna University Press, 2023; J-L. Alber, *Le droit douanier de l’Union européenne*, Brussels, Belgium, Bruylant, 1st ed., 2023.

In May 2023, the European Commission issued a proposal for an ambitious and wide-ranging reform of the EU Customs Union.⁵⁸ The Commission declared that these reforms are necessary in order to create an agile and future-proof Customs Union, ready for increased trade volumes and digital transitions. The most important amendments of the proposal include the establishment of an EU customs authority, with the task of overseeing a new EU customs data hub. This centralised data hub would serve as a single centralised IT environment and ensure the integrity, traceability and non-repudiation of the data submitted to or collected by the customs authorities, which should thus strengthen customs control and contribute to combatting customs fraud and smuggling.

1.5. Tax enforcement as regards VAT

The administrative sovereignty over taxation lies exclusively with Member States, with the EU generally not involved in ensuring compliance with tax law. However, the rise in mobility of taxpayers, the growth in cross-border transactions, as well as the internationalisation of financial instruments have posed significant challenges for Member States in properly assessing taxes owed.⁵⁹ These difficulties have affected the functioning of tax systems, inciting tax fraud and tax evasion, while the powers of controls remained at national level.⁶⁰ As a result, Member States have agreed to develop in-depth administrative cooperation between the tax authorities through the cross-border framework and instruments provided at the EU level.

In this context, a number of EU instruments have been adopted to facilitate and strengthen such cooperation between national tax administrations. That is the case, for instance, of Council Directive

⁵⁸ European Commission, *Communication from the Commission on Customs reform: Taking the Customs Union to the next level*, COM/2023/257 final, European Union, Brussels, 17.5.2023; European Commission, *Proposal for a Regulation of the European Parliament and of the Council establishing the Union Customs Code and the European Union Customs Authority, and repealing Regulation (EU) No 952/2013*, Communication, COM/2023/258 final, European Union, Brussels, 17.5.2023; European Commission, *Proposal for a Council Regulation amending Regulation (EEC) No 2658/87 as regards the introduction of a simplified tariff treatment for the distance sales of goods and Regulation (EC) No 1186/2009 as regards the elimination of the customs duty relief threshold*, COM/2023/259 final, European Union, Brussels, 17.5.2023; European Commission, *Proposal for a Council Directive amending Directive 2006/112/EC as regards VAT rules relating to taxable persons who facilitate distance sales of imported goods and the application of the special scheme for distance sales of goods imported from third territories or third countries and special arrangements for declaration and payment of import VAT*, COM/2023/262 final, European Union, Brussels, 17.5.2023.

⁵⁹ European Commission, *Proposal for a Council Directive on administrative cooperation in the field of taxation*, COM/2009/0029 final, Brussels, 2.2.2009.

⁶⁰ *Ibid.*

2011/16/EU,⁶¹ which establishes the rules and procedures under which the Member States are required to cooperate in order to exchange information that is relevant for the administration and enforcement of their respective domestic tax laws. Yet, the latter does not apply to value added tax (VAT).⁶²

1.6. GDPR enforcement

The GDPR adopts a decentralised enforcement model, meaning that it confers a specific role to national data protection authorities (DPAs) to enforce the application of data protection rules on their respective territories.⁶³ Still, although not providing for a specific legal basis for requesting data from private actors, the GDPR includes specific provisions regarding the investigative powers that national DPAs should be granted.

To this end, DPAs across Member States should have the same tasks and effective powers, including investigatory and corrective powers.⁶⁴ Member States should implement a system which provides for effective, proportionate and dissuasive penalties.⁶⁵ Corrective powers under the GDPR can range from issuing warnings and reprimands to ordering a definite ban on processing, and even imposing administrative fines, which, for especially severe violations, can reach up to 20 million euros or 4% of the company's total worldwide annual turnover.⁶⁶ In addition, the GDPR does allow Member States to impose other penalties for infringements of the Regulation.⁶⁷ The nature of such penalties, criminal or administrative, should be determined by the law of the Member State law, provided that they are 'effective, proportionate and dissuasive'.⁶⁸

In 2023, EU Member States imposed approximately 2.1 billion euros in fines for GDPR violations.⁶⁹ Notable cases include a 1.2 billion euros fine issued by the Irish DPA on Meta Platforms Ireland Ltd., and a fine of 746 million euros levied by the Luxembourg's National Commission for Data

⁶¹ Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, OJ L 64, 11.3.2011, pp. 1-12, recital 1.

⁶² *Ibid.*, Article 2.

⁶³ Article 57(1), GDPR.

⁶⁴ Article 58, GDPR.

⁶⁵ Recital 152, GDPR. P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*. Springer, Cham., 2017, DOI: https://doi.org/10.1007/978-3-319-57959-7_7.

⁶⁶ Article 83, GDPR.

⁶⁷ Article 84, GDPR.

⁶⁸ Recital 152, GDPR.

⁶⁹ European Data Protection Board, *EDPB Annual Report 2023*, EDPB, 2023; The Enforcement Tracker gives an overview of reported fines and penalties which data protection authorities within the EU have imposed so far, CMS law tax future, 'GDPR Enforcement tracker', online <https://www.enforcementtracker.com>.

Protection (CNPD) on Amazon, for misuse of customer data in targeted advertising.⁷⁰ Given the severity of these fines, there is little doubt that they may be considered as ‘punitive in nature’, as they are intended to act as a deterrent for companies from committing GDPR infringements. This interpretation seems to be confirmed by Advocate General Campos Sánchez-Bordona, who affirmed that, under the GDPR, ‘civil liability performs a ‘private’ compensatory function, whereas fines and criminal penalties are meant to have a public deterrent and, as the case may be, punitive function’.⁷¹ More recently, the ECJ has ruled that Articles 83 and 84 of the GDPR essentially serve a ‘punitive purpose’, ‘since they permit the imposition of administrative fines and other penalties’.⁷²

2. PUNITIVE ADMINISTRATIVE PROCEEDINGS: GENERAL FRAMEWORK

The action of EU institutions is inherently constrained by the obligation to adhere to the general principles of EU law. These general principles of law are one of the sources of EU law and possess a constitutional status. They largely derive from the fundamental values and constitutional traditions common to the national legal systems of the Member States.⁷³ Furthermore, the ECJ has explicitly recognised that the respect of fundamental rights granted by the EU legal order constitutes an integral component of the general principle of EU law.⁷⁴

General principles of EU law function as overarching legal criteria that guide and limit the exercise of powers conferred to them within the EU legal order, ensuring that their action aligns with the Treaties and the Charter. They also serve as benchmarks for reviewing the legality of acts adopted by EU institutions, as well as to establish a basis for their non-contractual liability under Article 340 TFEU.⁷⁵

While providing a comprehensive overview lies beyond the scope of this chapter, it suffices to highlight here that general principles of EU law include, *inter alia*, the principles of proportionality, non-discrimination, the protection of legitimate expectations, the right to good administration, as well

⁷⁰ *Ibid.*

⁷¹ ECJ, Opinion of Advocate General Campos Sánchez-Bordona, *UI v. Österreichische Post AG*, 04.05.2023, C-300/21, § 88.

⁷² ECJ, *GP v. Juris GmbH*, 01.12.2021, C-741/21 § 59

⁷³ T. Tridimas, *The General Principles of EU Law*, Oxford, United Kingdom, Oxford University Press, 3rd ed., 2006.

⁷⁴ ECJ, *Internationale Handelsgesellschaft*, 17.12.1970, C-11/70 and ECJ, *Nold*, 14.05.1974, C-4/73.

⁷⁵ H. Hofmann, ‘General Principles of EU law and EU administrative law’ in: S. Peers, C. Barnard (eds.), *European Union Law*, Oxford, United Kingdom, Oxford University Press, 2014.

as fundamental defence rights, including the right to be heard and the right to an effective judicial remedy.

By way of illustration, the principle of proportionality plays a key role in confining the actions taken by EU institutions within certain bounds. Under Article 5(4) TEU, the content and form of Union action must be limited to what is necessary for attaining the objectives set out in the Treaties. The principle of proportionality holds particular relevance to the subject matter of this Chapter, insofar as measures adopted by EU authorities cannot exceed what is appropriate and necessary to achieve the legitimately pursued objectives. The ECJ has further detailed the principle, clarifying that in case of choice between several measures, ‘recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued’.⁷⁶ Importantly, the principle of proportionality plays a crucial role when assessing the legality of limitations to fundamental right granted by the Charter.⁷⁷ The ECJ itself has consistently used the proportionality principle as a key legal standard for balancing individual rights against public interests, particularly in the context of criminal investigative measure involving interferences with the right to privacy and data retention regimes. In this context, the proportionality principle ensures a balance between investigatory measures deployed and the right of those affected by them, preventing overly intrusive interventions where less restrictive options can achieve the same goals.

Similarly, good administration has been recognised since the very early case law of the ECJ as a general principle of EU law and,⁷⁸ following the entry into force of the Charter, as a binding fundamental right.⁷⁹ It requires that ‘every person has his or her affair handled impartially and within a reasonable time’ by the Union’s institutions.⁸⁰ In this context, the ECJ has recognised that the principle of sound administration imposes a duty of care on the EU administration, which requires a thorough establishment of facts before taking any decisions. Key components of this right include the right to be heard, the right to have access to the file, as well the obligation of the administration to give reasons for its decisions.

As a result, when assessing the scope and exercise of powers by EU institutions, agencies, and bodies endowed with direct enforcement authority – particularly when such powers culminate in decisions adversely affecting individuals – it is imperative to take these general principles into account, and

⁷⁶ECJ, *Jippes v. Commission*, 12.07.2001, C-189/01, § 81.

⁷⁷ Article 52(1) Charter.

⁷⁸ Now codified in Article 6(3) TEU.

⁷⁹ Article 41 Charter.

⁸⁰ ECJ, *Agrobet CZ s.r.o. v. Finanční úřad pro Středočeský kraj*, 14.05.2020, C-446/18, § 43.

this regardless of whether these principles are explicitly mentioned in EU secondary law.

3. PUNITIVE ADMINISTRATIVE PROCEEDINGS: SECTORIAL FRAMEWORK

3.1. Requests for data to online service providers

3.1.1. Competition law enforcement

Regulation 1/2003 does not foresee among the powers of investigations granted to DG COMP a specific legal basis for requesting data from private actors, such as OSPs. The collection of data in administrative proceedings in the field of competition law remains still largely confined to traditional methods of evidence gathering. However, over time, DG COMP has already had, and will increasingly have, to adapt its traditional investigative powers to effectively deal with the current predominance of electronic evidence, keeping pace with a world where information is mostly produced and stored digitally.

First, to acquire information necessary for its investigation, DG COMP may issue requests for information, which are frequently employed following unannounced inspections under Article 20 of Regulation 1/2003.⁸¹ The general legal basis to request information is outlined in Article 18 of Regulation 1/2003. The latter provides that DG COMP may require ‘undertakings and associations of undertakings’ to provide ‘all necessary information’. In practice, such requests for information are regularly addressed not only to undertakings under investigation, but also to third parties, namely other undertakings which may be aware of information relevant for the case, irrespective of their involvement in the suspected infringement.⁸² While this category has traditionally been used to target customers, suppliers or competitors of the undertaking under investigation, as we will see, the broad formulation could lend itself to an evolutionary interpretation of the law, potentially extending to encompass OSPs as well.

Article 18 of Regulation 1/2003 expressly limits the scope of requests for information only to what is ‘necessary’. While determining what constitutes necessary information, DG COMP enjoys a wide margin of appreciation,⁸³ but in exercising its discretion, it remains bound by the

⁸¹ Jones, Sufrin, Dunne, (no.8).

⁸² European Commission, *Commission notice on best practices for the conduct of proceedings concerning Articles 101 and 102 TFEU*, EU, 20.10.2011, 2011/C 308/06, p.12, §. 32.

⁸³ ECJ, *Thyssen Stahl v. Commission*, 11.03.1999, T-141/94, § 110; ECJ, *HFB and Others v. Commission*, 20.03.2002, T-9/99, § 384; ECJ, *Corus UK v. Commission*, 08.07.2004, T-48/00, § 212.

principle of proportionality.⁸⁴ In this context, the ECJ has affirmed the need for a correlation between the request for information and the putative infringement.⁸⁵ Consequently, DG COMP may request information or documents only to the extent that a particular item is necessary to bring to light an infringement of competition rules.⁸⁶ Accordingly, DG COMP should only require the disclosure of information ‘which may enable it to investigate presumed infringements which justify the conduct of the investigation and are set out in the request for information’.⁸⁷ Although it may be difficult to prove that the Commission has exceeded its leeway, it is certainly precluded from issuing measures of an exploratory nature, so-called ‘fishing expedition’.⁸⁸

In practice, requests for information – contrary to inspections – are used to obtain specific ‘information to enable it better to define the scope of the infringement, to determine its duration or to identify the circle of undertakings involved’.⁸⁹ This includes requests for the production of documents, but also to answer questions relating to those documents. In this regard, it is settled case-law that documents of a non-business nature, meaning documents not relating to the market activities of the undertaking, are excluded from the scope of DG COMP investigatory powers.⁹⁰ Moreover, the Commission is prevented from including any questions which would compel the undertaking to provide answers that may entail an admission of guilt.⁹¹

Article 18 of Regulation 1/2003 distinguishes between a simple request for information⁹² and a formal Commission decision.⁹³ The undertaking concerned by a simple request for information does not have a duty to comply nor DG COMP can impose fines for non-compliance. Therefore, Article 18(2) may possibly serve as legal basis for voluntary cooperation with OSPs. Still, the Commission may impose fines where incorrect or misleading information

⁸⁴ Commission Notice on Best Practices, (no. 78), p. 13.

⁸⁵ ECJ, Opinion of Advocate General Jacobs, *SEP v. Commission*, 15.12.1994., C-36/92 P, § 21.

⁸⁶ ECJ, *SEP v. Commission*, 12.12.1991, T-39/90, § 25.

⁸⁷ ECJ, *HeidelbergCement AG v. European Commission*, 10.03.2016, C-247/14 P, § 23 as confirmed, more recently, in ECJ, *Meta Platforms Ireland v. Commission*, 24.05.2023, T-451/20 R and T-452/20 R. The two actions brought by Facebook Ireland claimed the unlawfulness of DG COMP requests for information insofar as they required to produce internal documents manifestly irrelevant for the investigations.

⁸⁸ ECJ, *Cementos Portland Valderriva v. Commission*, 14.03.2014, T-296/11; ECJ, *Deutsche Bahn AG and others v. European Commission*, 18.06.2015, C-583/13 P.

⁸⁹ ECJ, *Orkem v. Commission*, 18.10.1989, C-374/87, § 15.

⁹⁰ ECJ, *AM & S Europe v. Commission*, 18.05.1982, C-155/79, § 16; ECJ, *Roquette Frères*, 22.10.2002, C-94/00, § 45.

⁹¹ ECJ, *Orkem v. Commission*, (no. 85).

⁹² Article 18(2) Regulation 1/2003.

⁹³ Article 18(3) Regulation 1/2003.

is, intentionally or negligently, supplied.⁹⁴ However, addressees of a simple request for information may refuse to reply questions perceived as potentially self-incriminating and decide to refer the matter to the Commission's hearing officer.⁹⁵ In appropriate cases, the hearing officer may issue a reasoned recommendation on the applicability of the privilege against self-incrimination,⁹⁶ which must be taken into account in any subsequent decision made under Article 18(3).⁹⁷

Indeed, in the event of refusal to supply the requested information, DG COMP retains the option to issue a formal decision, obliging the undertaking to provide the requested information. Such decision can indicate or impose periodic penalty payments of up to the 5% of the average daily turnover per day to compel them to comply.⁹⁸ An undertaking is thus under an obligation to actively cooperate, with the exception that it cannot be forced to admit to having committed an infringement.⁹⁹ This was first established in *Orkem*,¹⁰⁰ where the ECJ confirmed that 'the Commission may not compel an undertaking to provide it with answers which might involve an admission on its part of the existence of an infringement which it is incumbent upon the Commission to prove'.¹⁰¹ However, the addressee of a request may still be required to respond to factual questions and to provide pre-existing documents, even where such information 'may be used to establish, against it or another undertaking, the existence of an anti-competitive conduct'.¹⁰² In this context, data could certainly be regarded as pre-existing documents, which means that OSPs would be in any event obliged to supply such data when requested.

To ensure that it does not exceed what is necessary, the request for information must provide the legal basis and the purpose of the request, as well as indicate what information is required and within which deadline. As for the 'purpose' of the request, the ECJ has clarified that this refers to the Commission's obligation to define the subject of its investigation, specifying the alleged infringement of competition rules being probed.¹⁰³ However, this

⁹⁴ Article 23 Regulation 1/2003

⁹⁵ The role and functions of the hearing officer are governed by Decision of the President of the European Commission of 13 October 2011 on the function and terms of reference of the hearing officer in certain competition proceedings (2011/695), OJ L275, pp. 29-37.

⁹⁶ *Ibid.*, Article 4(2)(b).

⁹⁷ Commission Notice on Best Practices, (no. 78), § 36.

⁹⁸ Article 24 Regulation 1/2003.

⁹⁹ Recital 23 Regulation 1/2003.

¹⁰⁰ ECJ, *Orkem v. Commission*, (no. 85).

¹⁰¹ *Ibid.*, § 35.

¹⁰² *Ibid.*, § 34.

¹⁰³ ECJ, *HeidelbergCement v. Commission*, 10.03.2016, C-247/14 P, § 20 and case-law cited therein. F. Carlori, G. Da Costa, 'Judgments in the Cement Case: Requirement for Greater

obligation does not encompass a requirement for the Commission to disclose to the addressee of a request all information in its possession as regards the suspected infringement, nor to provide a detailed legal characterisation of that infringement.¹⁰⁴

Moreover, since the action of EU institutions is bound by the respect of the general principles of EU law, DG COMP must state the reasons justifying its request for information with sufficient precision.¹⁰⁵ The general obligation to state specific reasons, which stems from the right to good administration, is ‘a fundamental requirement designed not merely to show that the request for information is justified, but also to enable the undertakings concerned to assess the scope of their duty to cooperate whilst at the same time safeguarding their rights of defence’,¹⁰⁶ as well as to allow the Court to exercise its power of review.¹⁰⁷ Likewise, it is settled case-law that requests for information must comply with the principle of proportionality, so that ‘the obligation imposed on an undertaking to supply information should not be a burden on that undertaking which is disproportionate to the needs of the inquiry’.¹⁰⁸

As regard the time-limit within which the information is to be provided, the ECJ has clarified that it must enable the undertaking concerned not only to provide its reply, but also to satisfy itself that the information supplied is complete, correct and not misleading.¹⁰⁹ In this regard, the Commission Notice on Best Practices states that the time-limit is set taking into account the length and complexity of the request. In general, it will be at least two weeks, but may be shorter (one week or less) if the scope of the request is limited.¹¹⁰ Furthermore, the ECJ has admitted that DG COMP may request the information to be provided in a highly specific, detailed format.¹¹¹ Also, Article 18(4) provides that lawyers may supply the information on behalf of the undertaking concerned, although the latter remain fully responsible if the

Clarity, Specificity, and Justification for Information Requests from the Commission’, *Journal of European Competition Law & Practice*, 2016, vol. 7, no. 7, p. 457, DOI: 10.1093/jeclap/lpw032.

¹⁰⁴ ECJ, *HeidelbergCement v. Commission*, (n. 83), § 21.

¹⁰⁵ According to Article 296 TFEU legal acts of EU institutions shall state the reasons on which they are based.

¹⁰⁶ ECJ, *HeidelbergCement v. Commission*, (no. 83), § 19; ECJ, *Meta Platforms Ireland Ltd v. Commission*, (no. 10), § 39.

¹⁰⁷ ECJ, *HeidelbergCement v. Commission*, (no. 83), § 24.

¹⁰⁸ ECJ, *Meta Platforms Ireland Ltd v. Commission*, (no. 10), § 269; ECJ, *SEP v. Commission*, (no. 82), § 51; ECJ, *Qualcomm and Qualcomm Europe v. Commission*, T-371/17, §§ 120 and 121.

¹⁰⁹ ECJ, *Schwenk Zement KG v European Commission*, T-306/1, para. 73.

¹¹⁰ European Commission, *Commission Notice on best practices for the conduct of proceedings concerning Article 101 and 102 TFEU*, § 38.

¹¹¹ ECJ, *Cementos Portland Valderriva v. Commission*, 14.03.2014, T-296/11, §§ 87-89.

information provided is incomplete, incorrect or misleading. Finally, DG COMP is required to forward a copy of the simple request or decision to the NCA of the Member State in whose territory the seat of the undertaking concerned is situated and the NCA of the Member State whose territory is affected.¹¹²

Addressees of a request for information by decision – but not by simple request – have the right to have the decision reviewed by the ECJ.¹¹³ However, doubts have been raised on the effectiveness of this remedy due to the lack of suspensory effect of actions for annulment. As a result, it is unlikely that the undertaking will receive a decision from the ECJ within the timeframe fixed by DG COMP for the collection of information.¹¹⁴

Yet, inspections remain at present the primary tool in the hands of DG COMP for gathering key evidence to establish competition law infringements. Article 20 of Regulation 1/2003 empowers DG COMP to conduct inspections at the premises of ‘undertakings and associations of undertakings’. At present, DG COMP’s authority to collect digital evidence stems from its existing power to examine all books and records of the undertaking under inspection, ‘irrespective of the medium on which they are stored’.¹¹⁵

The effectiveness of inspections is due to several factors. First, in its inspections, DG COMP applies the ‘access principle’, which grants inspectors the right to access all information that is accessible to the undertaking subject to the inspection. This principle applies irrespective of the location or ownership of the servers on which the data are stored. As a consequence, data stored on servers located anywhere are considered to be falling within the scope of the inspection, provided that the undertaking has access to them. Moreover, the undertakings’ duty of cooperation also implies the obligation to provide the so-called ‘administrator access rights’.¹¹⁶ Second, the destruction of documents poses significant risks on the undertaking and may lead to severe consequences, such as the imposition of fines or even constitute an aggravating factor in the assessment of the infringement. Moreover, the involvement of the Commission’s Forensic IT team during inspections not

¹¹² Article 18(5) Regulation 1/2003.

¹¹³ Article 18(3) Regulation 1/2003.

¹¹⁴ J. Fraga Nunes, ‘Electronic evidence in EU Competition Procedure: The need to reconcile the Commission’s investigatory powers with procedural defence and data protection rights’, *European Competition and Regulatory Law Review*, 2023, vol. 7, no. 1, p. 29.

¹¹⁵ Article 20(2)(b) Regulation 1/2003.

¹¹⁶ European Commission, *Explanatory note on Commission inspections pursuant to Article 20(4) of Council Regulation (EC) No 1/2003*, Revised in March 2024, § 11.

only ensures the chain of custody of evidence but also enables the recovery of delated data.¹¹⁷

Interviews with practitioners in the field seems to confirm this trend. None of the practitioners interviewed reported any instances where DG COMP had requested data or information from an OSP to establish the existence of a competition law infringement. Instead, it resulted that evidence is primarily gathered directly from the undertakings under investigations and suspected of the infringement. Furthermore, interviews revealed a continued preference for the collection of evidence directly from the undertakings under investigation, through the traditional investigative powers available to DG COMP, that is on-the-spot inspections and requests for information. This is due to the fact that, in most cases, evidence necessary to prove competition law infringements is typically held by, and thus more readily accessible though, the undertaking under investigation itself. As a result, the Commission can easily and more efficiently obtain the information needed by directly addressing the company suspected of the violation. Furthermore, DG COMP might still be able to gather the relevant evidence to prove the suspected infringement, for instance, through an inspection at the premises of a different undertaking that is somehow related to the suspected one.

Interviews further confirmed that electronic evidence is generally difficult to destroy, and that even deleted or damaged data can be retrieved. Even if a document on a digital medium is itself destroyed, a copy of it could be stored on another digital media or at least traces of its existence can be found, making its destruction relatively easy to detect. For this purpose, DG COMP inspection team includes IT experts equipped with forensic tools generally able to detect the deletion or manipulation of electronic information during inspections.

For instance, during the inspection at Nexans, DG COMP inspectors recovered from an employee's computer a number of files, documents and emails which had been deleted after the start of the investigation but considered relevant to the investigation.¹¹⁸ More recently, during another inspection, DG COMP imposed a fine of 15.9 million on a company for obstructing its inspection after detecting that an employee had intentionally deleted WhatsApp messages exchanged with a competitor that contained

¹¹⁷ OECD, *Investigative powers in practice – Breakout session 1 and Breakout session 3 – Contribution from the European Commission*, 30.11.2018, DAF/COMP/GF/WD(2018)(25), p. 4, § 5.

¹¹⁸ ECJ, *Nexans v. Commission*, 14.11.2012, T-135/09, § 12.

business-related information. In this instance as well, DG COMP successfully restored the deleted data.¹¹⁹

These cases show how DG COMP has both the technological tools and coercive powers to compel companies under investigation to cooperate in order to obtain evidence of anti-competitive behaviour, thus rendering the need to request data directly from the OSPs (such as WhatsApp in this case) unnecessary. However, given the rapid development of technological advancement, it is not excluded that in the future the need to obtain information directly from OSPs may arise, particularly where certain data cannot be otherwise obtained.

A potential solution to this issue could be offered by the use of requests for information. Indeed, Article 18 of Regulation 1/2003 concerning requests for information is worded broadly enough to potentially include OSPs within its scope. This general legal basis – which is currently used exclusively to request relevant information from undertakings involved in the suspected infringement – could therefore be interpreted in a way to allow DG COMP to address its requests for information directly to OSPs. This view has also been considered plausible by practitioners in the field, who have emphasised how the main feature of Regulation 1/2003 – which has contributed to its success – is its broad formulation, which allows for a dynamic interpretation in line with the times. If this interpretation is adopted, however, additional safeguards may be necessary, especially depending on the type of data requested, such as the requirement for an *ex ante* judicial authorisation.

As the exercise of its investigative powers by DG COMP may constitute a significant intrusion into the private sphere of undertakings concerned, its action is subject to certain limitations and procedural safeguards aimed at preserving their rights of defence.

Although not expressly addressed in Regulation 1/2003, legal professional privilege (LPP) is recognised as a general principle of EU law, which preserves the confidentiality of certain communications between lawyer and its clients. According to the case law of ECJ, communications between a client and its lawyer are protected by LPP provided that they are made ‘for the purpose and interest of the exercise of the client’s rights of defence’ in competition proceedings and that they emanate from ‘independent lawyers’.¹²⁰ Nor, as mentioned above, does the duty to cooperate with the

¹¹⁹ European Commission, *Commission fines International Flavors & Fragrances & Fragrances €15.9 million for deleting WhatsApp messages during an antitrust inspection*, Press Release, 24.06.2024.

¹²⁰ ECJ, *AM & S v. Commission*, 18.05.1982, C-155/79, §§ 21-24.

Commission mean that the undertaking is required to incriminate itself.¹²¹ However, while the privilege against self-incrimination is particularly significant for the protection of undertakings under investigation or other undertakings related to them, it might be less relevant for OSPs. This is because OSPs will normally be required to provide data concerning third parties and that exists/has been produced independently from their will. Yet, OSPs might still be demanded, for instance, to assess if data requested is protected by LPP.

Moreover, as part of their right of defence, after the notification of the statement of objection, the undertaking ‘which are subject to the proceedings’ must be given the opportunity of being heard on the matters to which DG COMP has taken objection. In this regard, DG COMP must base its decisions only on objections on which the parties concerned have been able to comment.¹²² Addressees of a statement of objection also have the right of access to the file, with the exception of internal documents and confidential information.¹²³

The Commission has a general duty to protect confidential information.¹²⁴ Accordingly, Article 28 of Regulation 1/2003, concerning professional secrecy, contains a limitation to the use of information collected by DG COMP in the course of its investigations. As clarified by the ECJ, such a requirement is aimed at preserving undertakings’ right of defence, which would be seriously endangered if DG COMP were to rely on evidence ‘which was obtained during an investigation but was not related to the subject-matter or purpose thereof’.¹²⁵ However, that does not prevent DG COMP from initiating a new investigation to verify or supplement information obtained during a previous investigation, should that information indicate the existence of anti-competitive practices.¹²⁶

Additionally, the ECJ has recognised a ‘very special protection’ to business secrets, meaning any information about an undertaking’s business

¹²¹ P. Van Cleynenbreugel, ‘The right to avoid self-incrimination: yet another elephant in the automated competition law enforcement room?’, *Jean Monnet Network on EU Law Enforcement Working Paper Series*, 2024, vol. 2024, no. 9(3), 2024-12, pp. 978-997; P. Van Cleynenbreugel, The Privilege against Self-Incrimination in EU Competition Law: Time for a Case Law Update?, *Bialystok Legal Studies*, 2023, vol. 28, no. 4, pp. 117-130.

¹²² Article 27(1) Regulation 1/2003.

¹²³ Article 27(2) Regulation 1/2003 and Article 15(1) and (2) of the Implementing Regulation. The practical arrangements are contained in the Commission Notice on the rules for access to the Commission file in cases pursuant to Articles 81 and 82 of the EC Treaty, OJ C 325, pp. 7–15.

¹²⁴ Article 339 TFEU.

¹²⁵ ECJ, *Deutsche Bahn v. Commission*, 18.06.2015, C-583/13 P, § 58.

¹²⁶ *Ibid.* § 59.

activity that if disclosed would cause a serious harm to the undertaking.¹²⁷ This protection covers also data collected from third parties.

Finally, the concentration of both investigative and decision-making powers within a single administrative authority has prompted concerns over whether such broad and far-reaching powers are adequately controlled.¹²⁸ Since Article 31 of Regulation 1/2003 affords the ECJ ‘unlimited jurisdiction’ to review final decisions of the Commission under Article 263 TFEU, this has generally been considered to be compatible with Article 6 of the ECHR, which requires for a fair and public hearing review by an independent and impartial tribunal.¹²⁹

3.1.2. Punitive enforcement in the area of banking law and financial markets

3.1.2.1. ECB

Under the SSM Regulation, the ECB is granted broad investigatory powers to collect relevant information necessary for fulfilling its supervisory duties.¹³⁰ These powers include the authority to request information,¹³¹ compel the production of documents, examine the books and records of supervised entities, obtain written and oral explanations, interview any persons who consent to do so,¹³² and carry out on-site inspections.¹³³

In particular, according to Article 10 of the SSM Regulation, the ECB may request to provide ‘all information that is necessary’ to carry out its tasks. Such requests, however, may only be addressed to the legal or natural persons listed therein. The latter are the entities that can be investigated by the ECB, namely credit institutions established in the Member States participating in the SSM, mixed financial holding companies and mixed-activity holding

¹²⁷ ECJ, *AKZO Chemie v. Commission*, 24.06.1986, C-53/85.

¹²⁸ A. Setari, *The standard of judicial review in EU competition cases: the possibility of introducing a system of more intense or full judicial review by the EU courts*, Tesi di Dottorato di Ricerca, Università degli Studi di Milano, 2014; D. Slater, S. Thomas, D. Waelbroeck, ‘Competition Law Proceedings before the European Commission and the Right to a Fair Trial: No Need for Reform?’, *GCLC Working Paper*, no. 04/08, 2005.

¹²⁹ ECJ, *KME Germany and Others v. Commission*, 08.12.2011, C-272/09 P; ECJ, *Chalkor v. Commission*, 08.12.2011, C-386/10 P; ECJ, *Schindler Holding Ltd and Others v. European Commission*, 18.07.2013, C-501/11 P, §§ 33-36; G. Muguet-Poullennec, ‘Sanctions prévues par le règlement no 1/2003 et droit à une protection juridictionnelle effective: les leçons des arrêts KME et Chalkor de la CJUE’, *Revue Lamy de la Concurrence: droit, économie, regulation*, 2012, no. 32, pp. 57-78.

¹³⁰ Articles 10-13, SSM Regulation.

¹³¹ Article 10, SSM Regulation.

¹³² Article 11, SSM Regulation.

¹³³ Article 12, SSM Regulation.

companies established in said States, persons belonging to these credit institutions or companies, and third parties to which these institutions or companies have outsourced functions or activities.¹³⁴ As it stands, the ECB may rely on this general legal basis to request data from OSPs only to the extent that the OSP itself qualifies as an ‘outsourcee’ according to Article 10(1)(f).¹³⁵

Upon a request to provide information, the addressees of such requests are under a legal obligation to comply, regardless of the existence of professional secrecy provisions (including banking secrecy).¹³⁶ While the SSM Regulation itself does not explicitly address legal profession privilege, Recital 48 acknowledges it as a ‘fundamental principle of Union law, protecting the confidentiality of communications between natural or legal persons and their advisors’,¹³⁷ as such fully applicable in accordance with the conditions laid down in the ECJ case-law.

The launch of an investigation must be preceded by an ECB decision.¹³⁸ Such a decision shall indicate its legal basis and purpose, the intention to exercise the general investigatory powers laid down in Article 11(1) of the SSM Regulation, and highlight that any interference by the person being investigated constitutes a breach directly punishable by the ECB. Conversely, requests for information pursuant to Article 10 of the SSM do not require the prior issuance of an ECB decision.¹³⁹ In such cases, the ECB is only required to detail the information sought and fix a reasonable deadline for its submission.¹⁴⁰ Additionally, the ECB must ensure that a copy of the information received is shared with the relevant NCA.¹⁴¹

Article 126 of the SMM Framework Regulation is devoted to the procedural rights granted to the supervised entity concerned in case of the imposition of administrative penalties. As a result, they should be applicable solely to the supervised entity concerned and not to OSPs as the addressees of information requests. These procedural guarantees include, *inter alia*, the right to be informed,¹⁴² the right to submit written observations,¹⁴³ the right to attend an oral hearing convened at the initiative of the Investigating Unit, with the assistance of a lawyer or other qualified individuals,¹⁴⁴ and the right

¹³⁴ Article 10(1), SSM Regulation.

¹³⁵ Any third parties to whom the supervised entities have outsourced functions or activities.

¹³⁶ Article 10(2), SSM Regulation.

¹³⁷ Recital 48, SSM Regulation.

¹³⁸ Article 142, SSM Framework Regulation.

¹³⁹ Article 139, ECB Regulation 468/2014.

¹⁴⁰ *Ibid.*

¹⁴¹ Article 139(3) ECB Regulation 468/2014.

¹⁴² Article 126(1), SMM Framework Regulation.

¹⁴³ Article 126(2), SMM Framework Regulation.

¹⁴⁴ Article 126(3), SMM Framework Regulation.

of access to the file.¹⁴⁵ Notably absent is the right not to incriminate oneself, as codified by the ECJ in the *Orkem* case in the area of competition law, which ought to be equally applicable in the banking sector as regards ‘punitive’ penalties.¹⁴⁶

Within the framework of the SSM, decision adopted by the ECB, which are of supervisory nature (such as those concerning investigatory measures or the imposition of penalties) are subject, firstly, to optional internal administrative review carried out by the Administrative Board of Review (ABoR), without prejudice to the right to seek judicial review before the ECJ under Article 263 TFEU.¹⁴⁷ Moreover, the ECB can be held liable for damages pursuant to Article 340 TFEU.¹⁴⁸

In conclusion, Article 10 of the SSM Regulation defines its personal scope of application in a way that restricts the potential addressees of ECB requests for information exclusively to supervised credit institutions and, in case of third parties, only to those to which supervised entities have outsourced functions or activities. Accordingly, a literal interpretation of this general legal basis would preclude an application of the provision to OSPs, unless they qualify as an ‘outsourcee’.

3.1.2.2. ESMA

A specific legal basis to request ‘records of telephone and data traffic’ is provided to ESMA under several sectorial instruments.¹⁴⁹ These provisions grant ESMA the power to obtain such data from the entities under its supervision, ensuring that relevant information can be gathered to assess compliance with EU financial regulations. However, these powers are restricted in their personal scope, as they only apply to specific private actors, primarily supervised entities. Under Article 23c(1) of the Regulation on credit rating agencies (CRAR), ESMA can conduct necessary investigations into persons referred to in Article 23b(1), which concerns requests for information. These persons include CRAs, individuals involved in credit rating activities, rated entities and related third parties, and third parties to

¹⁴⁵ Article 126(4), SMM Framework Regulation and Article 32 SSM Framework Regulation.

¹⁴⁶ S. Allegrezza, O. Voordeckers, *Investigative and Sanctioning Powers of the ECB in the Framework of the Single Supervisory Mechanism*, eucrim, no. 4/2015, Max Planck Institute for the Study of Crime, Security and Law, 2015, pp. 151-161.

¹⁴⁷ For a more in-depth analysis of remedies against acts and decision adopted by the ECB within the SSM, see O. Voordeckers, ‘Administrative and Judicial Review of Supervisory Acts and Decisions under the SSM’, in S. Allegrezza (ed.), *The Enforcement Dimension of the Single Supervisory Mechanism*, Milan Italy, Wolters Kluwer, 2020, pp.93-130.

¹⁴⁸ Recital 61 SSM Regulation.

¹⁴⁹ Respectively, Article 23c(1)(e) of the CRAR, Article 25g(1)(e) and 62(1)(e) of the EMIR, Article 38c(1)(e) of the MIFIR and Article 48c(1)(e) of the Benchmark Regulation.

whom operational functions have been outsourced.¹⁵⁰ Also, the scope extends to ‘persons otherwise closely and substantially related or connected to credit rating agencies or credit rating activities’.¹⁵¹ Similarly, Article 48c(1)(e) of the Benchmark Regulation admits the possibility to request records of telephone and data traffic from persons involved in the provision of benchmarks, third parties to whom they have outsourced functions or activities, as well as ‘persons otherwise closely and substantially related or connected’ to them. By contrast, the Regulation on trade repositories (EMIR) limits the scope of application of such requests to trade repositories and the third parties to whom they have outsourced operational functions.¹⁵² Similarly, under Regulation 600/2014 (MiFIR), ESMA’s may only request supervised data reporting services providers, the persons that control them or are controlled by them, their managers, auditors or advisors.¹⁵³ The broader scope of application of CRAR and the Benchmark Regulation, which encompasses any other individual ‘closely and substantially related’ to the credit rating or benchmark provision process, reflects the necessity of extending oversight beyond just the core entities involved. However, it appears unlikely that these provisions could be interpreted to allow ESMA to request records of telephone and data traffic directly to OSPs. Interviews revealed that electronic evidence in ESMA investigations is predominantly performed via supervised entities rather than from third parties.¹⁵⁴

The specific type of data that ESMA may request are ‘records of telephone and data traffic’.¹⁵⁵ Importantly, these requests do not cover the actual content of communications but focus on traffic data such as call logs, connection records, or other metadata which can provide critical insights during investigations into market abuse, financial manipulation, or other infringements of financial regulations.

ESMA’s investigations are subject to several procedural safeguards, including the requirement to exercise its powers upon production of a written authorisation, specifying the purpose and subject-matter of the investigation.¹⁵⁶ Such written authorisation serves as a check against arbitrary requests, ensuring that data collection is conducted in line with the principles of necessity and proportionality. Moreover, ESMA’s powers cannot be used

¹⁵⁰ Article 23b(1), CRAR.

¹⁵¹ *Ibid.*

¹⁵² Article 25g(2) and 62(1) EMIR.

¹⁵³ Article 38b(1) MiFIR.

¹⁵⁴ Amandine Zelenko, Head of Enforcement Unit (ESMA).

¹⁵⁵ Article 23c(1)(e) CRAR, Article 25g(1)(e) and 62(1)(e) EMIR, Article 48c(1)(e) Benchmark Regulation, Article 38c(2) MiFIR.

¹⁵⁶ Article 23c(2) CRAR, Article 25g(2) and 62(2) EMIR, Article 48c(2) Benchmark Regulation, Article 38c(1)(e) MiFIR.

to require the disclosure of information or documents which are subject to legal privilege.¹⁵⁷

In addition, requests for records of telephone or data traffic may be subject to both *ex ante* (national) and *ex post* judicial review (European). If national law requires so, ESMA must apply for judicial authorisation from the competent national authority.¹⁵⁸ The national judicial authority is responsible for ensuring that ESMA's request is proportionate and necessary. However, the judicial review does not extend to questioning the overall necessity of the investigation, which remains within ESMA's discretion. Only the ECJ can ultimately assess the legality of ESMA's decision.

To compel the submission of requested data, ESMA may levy periodic penalty payments amounting to 3% of the average daily turnover in the preceding business year on non-cooperating entities.¹⁵⁹ This mechanism serves as an effective tool for enforcing compliance, particularly when entities are reluctant to cooperate or when the information provided is incomplete.

The legal framework governing ESMA's investigations includes several provisions aimed at safeguarding the defence rights of the entities concerned (though they do not extend to third parties not subject to the investigation). First, the persons subject to investigation must be given the opportunity to be heard before any findings are submitted to ESMA's Board of Supervisors.¹⁶⁰ In addition, they have the right of access to the investigation file, subject to limitations stemming from the protection of business secrets and confidential information affecting third parties.¹⁶¹ Decisions of ESMA to request telephone or data traffic records are subject to the legal remedies available under the ESMA Regulation.¹⁶² As a result, any natural or legal person may appeal against a decision of the ESMA which is addressed to that person, or against a decision which, although addressed to another person, is of direct and individual concern to that person before the Board of Appeal.¹⁶³ Any decision of the Board of Appeal can then be further challenged before the ECJ.¹⁶⁴

In addition to the above-mentioned specific legal basis to request records of telephone and data traffic, the sectoral legal framework provides ESMA with a general power to request information during its

¹⁵⁷ Article 23a CRAR, Article 60 EMIR, Article 48a Benchmark Regulation, Article 38a MiFIR.

¹⁵⁸ Article 23c(5) CRAR, Article 62(5) EMIR, Article 48(c)(5) Benchmark Regulation.

¹⁵⁹ Article 36b CRAR, Article 66 EMIR, Article 48g Benchmark Regulation, Article 38i MiFIR.

¹⁶⁰ Article 23e(3) CRAR and Article 64(3) EMIR.

¹⁶¹ Article 23e(4) CRAR and Article 64(4) EMIR.

¹⁶² Chapter V ESMA Regulation.

¹⁶³ Article 60, ESMA Regulation.

¹⁶⁴ Article 61, ESMA Regulation.

investigations.¹⁶⁵ Such provisions are identical in the substance and will therefore be examined together. The personal scope of ESMA's power to request information is the same as outlined above for requests of records of telephone and data traffic, thus the same considerations apply.¹⁶⁶ Information may be requested either through a simple request or a formal decision, with the latter granting ESMA the authority to impose periodic penalty payments to compel the entities concerned to provide the requested information.¹⁶⁷ After issuing a request, ESMA must inform the competent authority of the Member State where the private actor is domiciled or established, which ensures a level of transparency and national oversight over the investigation process.¹⁶⁸

Interviews indicated that this currently constitutes the predominant method by which ESMA acquires data during its investigations. In practice, ESMA primarily requires electronic evidence in the form of content data (e.g., emails, chats, documents). Data traffic information is infrequently employed, as ESMA's direct enforcement activity typically do not focus on tracing market abuse like infringements. The latter, by their nature, require traffic data to establish or exclude connections between different persons or identify networks of individuals involved. Instead, ESMA's investigations primarily focus on content information, precisely to verify the substance of the exchanges, rather than identifying the parties involved or the timing of the exchanges.¹⁶⁹

Moreover, several EU regulations foresee the power to request data among the investigative powers which should be conferred upon national competent authorities in the field of financial supervision. The MAR provides for comprehensive and directly applicable at national level regime of administrative enforcement, with far-reaching supervisory and investigative powers for NCAs.¹⁷⁰ Certain of these powers resemble to those traditionally exercised by judicial authorities.¹⁷¹ For instance, NCAs may compel the production of existing recordings of telephone conversations, electronic communications or traffic data held by investment firms, credit institutions or

¹⁶⁵ Respectively, in Article 23b CRAR, Article 25f and Article 61 EMIR, as well as Article 38b MiFIR and Article 48b of the Benchmark Regulation.

¹⁶⁶ Article 23b CRAR and Article 61 EMIR.

¹⁶⁷ Article 36b CRAR and Article 66 EMIR.

¹⁶⁸ Article 23b(5) CRAR and Article 61(5) EMIR.

¹⁶⁹ Interview with Christophe Polisset, Senior Officer in Investigations Unit, ESMA, 25.10.2024.

¹⁷⁰ *Ibid.*

¹⁷¹ V. Franssen, S. Vandeweerd, 'Supranational Administrative Criminal Law', *Revue Internationale de Droit Pénal*, 2019, vol. 90, no. 2, pp. 13-83.

financial institutions.¹⁷² Similarly, under certain circumstances,¹⁷³ the MAR allows competent authorities to request existing data traffic records ‘held by a telecommunications operator’.¹⁷⁴ These tools are crucial for investigating market abuse, where timely access to personal data is essential.¹⁷⁵ According to ESMA, the low number of sanctions under MAR is due, in part, to the difficulty in investigating and prosecuting market abuse, which often depends on prompt access to personal data, especially traffic data.¹⁷⁶ Following ESMA’s Opinion, traffic data are essential for NCAs to establish – or conversely to rule out – links among individuals potentially implicated in insider dealing cases, where circumstantial evidence plays a decisive role.¹⁷⁷ While traffic data does not reveal the content of the communications, it might provide indications of interpersonal connections that may suggest exchanges of inside information, thereby orienting the investigative efforts of NCAs.¹⁷⁸

A trend towards the inclusion of similar powers for NCAs can be observed in various other EU instruments in the field. As noted, these provisions aim at introducing a ‘level playing field’ across the Union regarding the access to telephone records and existing traffic data held by a telecommunication providers, as well as recordings of telephone conversations and traffic data retained by investment firms.¹⁷⁹ Such data often serve as crucial, if not the sole, evidence to identify and substantiate instances of market abuse, as well as to assess firms’ adherence to investor protection standards and other obligations set forth under relevant EU sector-specific legislation.¹⁸⁰ That is the case, for instance, of the AIFM Directive,¹⁸¹ which provides for the power to require ‘existing telephone and existing data traffic records’.¹⁸² MiFID II¹⁸³ provides instead that NCAs shall be given the power to request not only ‘existing recordings of telephone conversations or

¹⁷² Article 23(2)(g), MAR.

¹⁷³ Article 23(2)(h), MAR.

¹⁷⁴ Article 23(2)(h), MAR.

¹⁷⁵ ESMA, *Opinion on the European Commission’s proposed amendments to the draft Implementing Technical Standards on the precise format of insider lists and for updating insider lists adopted under MAR*, EU, 29.04.2022, ESMA70-449-501, § 38.

¹⁷⁶ *Ibid.*, § 37-38.

¹⁷⁷ *Ibid.*, § 39.

¹⁷⁸ *Ibid.*, § 40.

¹⁷⁹ Recital, 144, MiFID II.

¹⁸⁰ Recital 65 MAR; Recital 144 MiFID II.

¹⁸¹ Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010, OJ L 174, 1.7.2011, pp. 1–73.

¹⁸² Article 46(2)(d), AIFM Directive.

¹⁸³ Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, OJ L 173, 12.6.2014, pp. 349–496.

electronic communications or other data traffic records’ held by investment firms,¹⁸⁴ but also existing traffic data ‘held by a telecommunication operator’, subject to national law. This power applies where there is reasonable suspicion of a violation and such records may be relevant to the investigation.¹⁸⁵ However, such access excludes ‘the content of voice communications by telephone’.¹⁸⁶ Likewise, under the UCITS Directive,¹⁸⁷ competent authorities may require ‘existing data traffic records held by a telecommunications operator’ if there is reasonable suspicion of infringement breach and the data is relevant to the investigation of such infringement.¹⁸⁸

3.1.3. Customs enforcement

There are no EU-level legal provisions entrusting national customs authorities with the power to request data directly from OSPs in their administrative proceedings. The only general provision relevant to the matter can be found in Article 15 of Regulation 952/2013 establishing the Union Customs Code.¹⁸⁹ It relates to the ‘Provision of information to the customs authorities’ and mandates that any individual directly or indirectly involved in customs procedures or controls must, upon request and within the specified timeframe, supply all necessary documents and information in an appropriate format, as well as offer any assistance needed to complete those formalities or controls.¹⁹⁰ However, the exact extent of this provision depends on how it has been transposed into national law by each Member States, which is subject to the analysis in the subsequent national chapters.

3.1.4. Tax enforcement as regards VAT

Interestingly, Article 249 of the EU VAT Directive,¹⁹¹ which concerns the right of tax authorities to access invoices stored by electronic means in another Member State, specifically grants national tax authorities the power to ‘access, download and use electronically stored invoices for control purposes’. This right applies both to the Member State where the taxable

¹⁸⁴ Article 69(2)(d), MiFID II.

¹⁸⁵ Article 69(2)(r), MiFID II.

¹⁸⁶ Recital 65 MAR; Recital 144 MiFID II.

¹⁸⁷ Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS), OJ L 302, 17.11.2009, pp.32-96.

¹⁸⁸ Article 98, UCITS Directive.

¹⁸⁹ Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code, OJ L 269, 10.10.2013, pp. 1–101.

¹⁹⁰ *Ibid.*, Article 15.

¹⁹¹ Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, OJ L 347, 11.12.2006, pp. 1–118.

person is established and to any other Member State where VAT is due, provided that the storage method ensures online access to the relevant data. However, the Directive does not explicitly address the question whether tax authorities could directly request invoices from the OSP hosting the data in cases where the taxable entity cannot provide such access or refuse to do it. This raises questions on the extent to which tax authorities can engage directly with third-party OSPs for VAT enforcement purposes.

Despite the absence of a centralised VAT enforcement at the EU level, the ECJ has produced an extensive body of case law concerning the protection of individuals' rights in national VAT proceedings. First, the right to good administration, enshrined in Article 41 of the Charter, has been recognised as a general principle of EU law that applies also to VAT enforcement proceedings.¹⁹² This right guarantees that any administrative procedure must be conducted fairly, impartially, based on 'the most complete and reliable information possible',¹⁹³ and within a reasonable time frame.¹⁹⁴ Additionally, based on Article 47 of the Charter, which protects the right to an effective remedy and to a fair trial, the ECJ has recognised that the parties should 'be able to debate and be heard on the matters of fact and of law which will determine the outcome of the proceedings'.¹⁹⁵ In particular, the court should be able to verify the legality of the evidence gathered in and transferred from related administrative procedures initiated by the same authority in relation to different taxpayers,¹⁹⁶ and to disregard any evidence deemed unlawful.¹⁹⁷ The respect for the rights of defence, as a general principle of EU law applicable to VAT enforcement,¹⁹⁸ further ensures that any affected person must be granted the opportunity to be heard during the administrative procedure and before an administrative decision is adopted.¹⁹⁹ Finally, the ECJ case law underscores the right of access to the file, unless the legitimate interests of confidentiality and of professional and business secrecy require

¹⁹² See, for instance, ECJ, *Agrobet CZ s.r.o. v. Finanční úřad pro Středočeský kraj*, (no.76), § 43.

¹⁹³ *Ibid.*, § 44.

¹⁹⁴ ECJ, *Napfény-Toll Kft. v. Nemzeti Adó- és Vámhivatal Fellebbviteli Igazgatósága*, 13.07.2023, C-615/21, § 53.

¹⁹⁵ ECJ, *Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres*, 28.07.2016, C-543/14, § 41; ECJ, *Glencore Agriculture Hungary Kft v. Nemzeti Adó- és Vámhivatal Fellebbviteli Igazgatósága*, 16.10.2019, C-189/18, § 62; ECJ, *Aquila Part Prod Com SA v. Nemzeti Adó- és Vámhivatal Fellebbviteli Igazgatósága*, 1.12.2022, C-512/21, § 60.

¹⁹⁶ *Ibid.*, *Glencore Agriculture Hungary Kft*, § 67.

¹⁹⁷ ECJ, *WebMindLicenses kft v. Nemzeti Adó- és Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, 17.12.2015, C-419/14, § 89; *Ibid.*, *Glencore Agriculture Hungary Kft*, § 68.

¹⁹⁸ *Ibid.*, *WebMindLicenses*, § 84.

¹⁹⁹ ECJ, *Glencore Agriculture Hungary Kft*, (no.188), § 41; ECJ, *SC CF SRL v. AJFPM and DGRFPC*, 4.06.2020, C-430/19, § 30.

otherwise.²⁰⁰ In such cases, the tax authority should nonetheless consider partial access to the file.²⁰¹

3.1.5. GDPR enforcement

As previously mentioned, the GDPR is primarily enforced at national level by national DPAs. Each Member State applies its own procedural and administrative rules to their GDPR enforcement procedures.²⁰² Nonetheless, the GDPR lays down the general framework regarding the DPAs' competence, tasks and powers. In particular, Article 58 lays down a wide range of investigative powers which should be conferred upon each national DPA. Such investigative powers include, *inter alia*, the power of DPAs to order the controller and the processor 'to provide any information it requires for the performance of its tasks';²⁰³ 'to obtain from the controller and the processor access to all personal data and all information necessary for the performance of its tasks';²⁰⁴ and 'to obtain access to any premises of the controller and the processor'.²⁰⁵ Hence, the GDPR provides for a broad legal basis for supervisory authorities to request or access information, which may include also data. Yet, the exercise of these powers seems limited in scope only to the controller and the processor under investigation. However, the GDPR does allow Member States to expand the investigative powers conferred on them by the Regulation.²⁰⁶ That is already the case in a number of Member States.²⁰⁷ The ECJ confirmed this extensive approach, clarifying that investigatory powers of national supervisory authorities, which constitute necessary means to perform their duties, are listed on a 'non-exhaustive' basis.²⁰⁸ Moreover, the data protection framework has traditionally been characterised by an expansive scope of application.²⁰⁹ The ECJ has justified such an extensive interpretation in order to ensure 'effective and complete' data protection for individuals.²¹⁰ Hence, national legislation that establishes

²⁰⁰ ECJ, *Teodor Ispas and Anduța Ispas v. Direcția Generală a Finanțelor Publice Cluj*, 9.11.2017, C-298/16, §§ 32-39; *Ibid.*, *SC CF SRL*, § 31.

²⁰¹ ECJ, *Glencore Agriculture Hungary Kft*, (no. 188), § 56.

²⁰² See National Reports.

²⁰³ Article 58(1)(a), GDPR.

²⁰⁴ Article 58(1)(e), GDPR.

²⁰⁵ Article 58(1)(f), GDPR.

²⁰⁶ Article 58(6), GDPR.

²⁰⁷ See, for example, A. De Vries, L. Mustert, M. Luchtman, A. Duijkersloot, And R. Widdershoven, The Netherlands, in this volume.

²⁰⁸ Although with reference to Article 28(3) of Directive 95/46. ECJ, *Maximillian Schrems v. Data Protection Commissioner*, 06.10.2015, C-362/14, § 43.

²⁰⁹ O Lynskey, 'Complete and Effective Data Protection', *Current Legal Problems*, 2023, vol. 76, no. 1, pp. 297–344, DOI: 10.1093/clp/cuad009.

²¹⁰ ECJ, *Google Spain v. AEPD and Mario Costeja González*, 14.05.2014, C-131/12, § 34.

a specific legal basis for requesting data from OSPs, or allows for a broad interpretation of a more general legal basis, should, under certain conditions, be deemed consistent with EU law.

Article 31 of the GDPR requires the controller, the processor and, where applicable, their representatives to cooperate with the supervisory authority upon request.²¹¹ Such provision must be read in conjunction with Recital 82 which imposes on controller and processor an obligation to cooperate with the supervisory authority and provide access to records when requested.²¹² Additionally, investigatory powers related to accessing premises must comply with specific procedural requirements established under Member State law, including the necessity of obtaining a prior judicial authorisation.²¹³

The exercise of powers by DPAs must adhere to appropriate procedural safeguards established under both Union and Member State law, ensuring actions are conducted ‘impartially, fairly and within a reasonable time’.²¹⁴ In particular, each measure should be ‘appropriate, necessary and proportionate’ to securing compliance with the GDPR, taking into considerations the specific circumstances of each case, respecting the right to be heard and avoiding unnecessary costs and burdens for the persons involved.²¹⁵ In addition, all legally binding measures of national DPAs must be in writing, presented clearly and unambiguously, indicate the issuing supervisory authority, the date of issuance, be signed by the head, or an authorised, state the reasons for the measure, and include information on the right of an effective remedy.²¹⁶ However, Member States’ procedural law may provide for additional requirements. The adoption of a legally binding decision implies the right to an effective judicial remedy in the Member State of the DPAs that adopted the decision.²¹⁷

The EU Agency for Fundamental Rights (FRA) has recently released a report on the experiences, challenges and practices identified by DPAs in the implementation of the GDPR, complementing the Commission’s forthcoming evaluation of the GDPR.²¹⁸ The report highlights the importance of a

²¹¹ C. Kuner, and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary*, New York, 2020, online edn, Oxford Law Pro.

²¹² Recital 82, GDPR.

²¹³ Recital 129 GDPR.

²¹⁴ *Ibid.*

²¹⁵ *Ibid.*

²¹⁶ *Ibid.*

²¹⁷ Article 78, GDPR.

²¹⁸ FRA, *GDPR in practice – Experiences of data protection authorities*, EU, 11.06.2024, p. 4. Between June 2022 and June 2023, FRA undertook 70 qualitative interviews with DPA representatives from all 27 EU Member States. ‘Interviewees were questioned on their experiences in the following areas: DPAs’ independence; the institutional capacity of DPAs;

thorough investigation, as precondition for effective enforcement. However, interviewees stressed various obstacles that hinder DPAs from performing their investigatory duties effectively. Several respondents suggested that investigatory measures listed in Article 58 of the GDPR are generally adequate but recommended complementing them with more sophisticated technical tools to enhance their enforcement capabilities. For instance, the use of undercover investigations, subject to appropriate safeguards, could enable DPAs to gather information while maintaining anonymity.²¹⁹ Further challenges identified include difficulties associated with assessing and admitting electronic evidence obtained during investigations.²²⁰ Another recurring challenge mentioned by interviewees concerns the reluctance of data controllers to cooperate with DPAs during investigations, a situation often attributed to the absence of mandatory cooperation obligations in numerous Member States.²²¹

Notably, the report does not address the issue of DPAs obtaining data directly from OSPs. One possible interpretation is that accessing OSP data is currently neither a common practice nor a significant concern among DPAs. This may reflect the fact that such access falls outside the typical scope of DPAs' investigatory powers under the GDPR, which focus more on compliance and cooperation with data controllers than on direct data extraction from third-party services. The legal framework might not sufficiently empower DPAs to compel disclosure from OSPs, particularly when the data in question pertains to users or systems not under direct investigation. Furthermore, the omission could suggest that, in practice, DPAs rely heavily on the cooperation of data controllers themselves and on-site inspections rather than acquisition of data from OSPs.

4. TRANSFER OF DATA BETWEEN PROCEEDINGS

4.1. Transfers of data between EU and national proceedings

National authorities may be required to exchange information with EU authorities or authorities established in other Member States on the basis of sector specific EU legislation.

modern technological challenges; raising public awareness; the investigatory powers of DPAs; sanctioning GDPR violations; cooperation between EU DPAs and the GDPR consistency mechanism; cooperation with other national regulators; and the protection of personal data and competing fundamental rights.'

²¹⁹ *Ibid.*, p.8.

²²⁰ *Ibid.*

²²¹ *Ibid.*

4.1.1. Customs enforcement

In the realm of customs enforcement, Article 16 of the Union Customs Code mandates Member States and the Commission to collaborate in the creation, maintenance and use of electronic systems for the exchange and retention of information among customs authorities and with the Commission.²²² Moreover, Regulation 515/97,²²³ which governs mutual assistance among administrative authorities of the Member States and their cooperation with the Commission, affirms that information acquired through mutual assistance may be used as evidence in judicial proceedings.²²⁴ In particular, under Article 8, requested authorities must make available any information in its possession, ‘and particularly reports and other documents or certified true copies or extracts thereof, concerning operations detected or planned which constitute, or appear to the applicant authority to constitute, breaches of customs or agricultural legislation’.²²⁵ As a result, where a Member State’s customs authority suspects that data held by an OSP relates to customs or agricultural irregularities (e.g. contracts, documents, invoices shared via online platforms), it may reasonably make use of the mechanisms established under Regulation 515/97 to request that information from another Member State’s authority, particularly where the OSP is based there, provided that the national law of the requested Member State permits it. Once the data is obtained and transmitted through the mutual assistance provided in the Regulation, it can legally be used as evidence in proceedings under Article 12, which provides that any documents or information obtained by the staff of the requested authority and communicated to the applicant authority may be invoked as evidence by the competent bodies of the Member States of the applicant authority²²⁶

4.1.2. Tax enforcement as regards VAT

The transfer of information between VAT authorities is covered instead by Council Regulation 904/2010 on administrative cooperation and combating fraud in the field of VAT.²²⁷ The latter lays down the conditions under which the competent authorities in the Member States responsible for

²²² Article 16 Regulation (EU) No 952/2013.

²²³ Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, OJ L 82, 22.3.1997, pp. 1–16.

²²⁴ Article 16 Regulation 515/97.

²²⁵ Article 8 Regulation 515/97.

²²⁶ Article 12 Regulation 515/97.

²²⁷ Council Regulation (EU) No 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax, OJ L 268, 12.10.2010, pp. 1–18.

the VAT enforcement are to cooperate with each other and with the Commission to ensure compliance with the law.²²⁸ To that end, it contains specific provisions regarding the rules and conditions under which competent authorities are to exchange information with each other.²²⁹

Regulation 904/2010 provides the possibility for tax authorities of a Member State (the requesting authority) to obtain information, and request specific administrative enquiries, from tax authorities of other Member State (the requested authority).²³⁰ However, it does not allow Member States to request administrative enquiries which would not be authorised ‘for that Member State’s own purposes’.²³¹ Administrative enquiries are broadly defined as ‘all the controls, checks and other action taken by Member States in the performance of their duties with a view to ensuring proper application of VAT legislation’.²³² Such enquiries are meant to gather ‘any information that may help to effect a correct assessment of VAT, monitor the correct application of VAT, particularly on intra-Community transactions, and combat VAT fraud’.²³³

Therefore, where information – including data obtained from an OSP in the course of its own investigations – is already lawfully held by the requested authority, Regulation 904/2010 could serve as a legal basis for transferring that data to the requesting authority, provided that relevant provisions of national law are observed. In this way, while the Regulation does not create new powers to compel OSPs to disclose information directly, it does enable the cross-border exchange of existing data, including that originating from OSPs, between competent tax authorities.

The provision of requested information may be refused where compliance would result in the disclosure of a commercial, industrial or professional secret, a commercial process, or information the disclosure of which would be contrary to public policy.²³⁴ Conversely, the Regulation does not admit a refusal to supply information based on banking secrecy.²³⁵

Regulation 904/2010 requires that the request for administrative cooperation be subsidiary, meaning that they should be made only after the

²²⁸ Article 1 Regulation 904/2010.

²²⁹ Chapter II, Exchange of information on request. Under Article 3 of the Regulation, each Member State must inform the Commission of the competent authorities responsible for exchanging information. The Commission provides Member States with a list of these competent authorities and publishes its content in the Official Journal of the European Union.

²³⁰ Article 7 Regulation 904/2010.

²³¹ Article 54(2) Regulation 904/2010.

²³² Article 2(1)(k) Regulation 904/2010.

²³³ Article 1(1) Regulation 904/2010.

²³⁴ Article 54(4) Regulation 904/2010.

²³⁵ Article 54(5) Regulation 904/2010.

requesting authority has exhausted the usual sources of information.²³⁶ Furthermore, the request should not impose a disproportionate administrative burden on the national tax authority.²³⁷ In principle, the request must be sent using a standard form,²³⁸ in any language agreed between the requested and requesting authority. Regulation 904/2010 does not provide for sanctions nor remedies.²³⁹ Nor does it establish specific rules regarding the authorisation or control of such requests.

When answering the requests, the requested authority must communicate all relevant information in its possession, including the outcomes of administrative enquiries, in the form of reports, statements or other documents, as well as certified true copies or extracts thereof.²⁴⁰ Where feasible, information should be provided by electronic means.²⁴¹ The requested authority shall provide the requested information ‘as quickly as possible and no later than three months following the date of receipt of the request’,²⁴² unless the information is already in its possession²⁴³ or otherwise agreed.²⁴⁴

Information transferred according to Regulation 904/2010 is subject to the obligation of official secrecy and must be used solely for the administrative and criminal purposes defined therein,²⁴⁵ unless the requested Member State allows its use for other purposes in accordance with its national law.²⁴⁶ Furthermore, all storage, processing and exchange of information under Regulation 904/2010 must adhere to the applicable data protection regulations. However, Member States are permitted to limit the rights of the data subject to ensure the effective performance of their tasks or that the prevention, investigation and detection of tax evasion and tax fraud is not jeopardised.²⁴⁷

²³⁶ Article 54(1)(b) Regulation 904/2010.

²³⁷ Article 54(1)(a) Regulation 904/2010.

²³⁸ Article 8 Regulation 904/2010.

²³⁹ J. Carbiener, S. Hiscock, ‘L’échange d’informations en matière de TVA et d’impôts directs : entre différences et convergences’, *Revue de Droit Fiscal*, 2020, vol. 6, p. 5.

²⁴⁰ Article 9(1), Regulation 904/2010.

²⁴¹ Article 51(1), Regulation 904/2010. For instance, the Regulation creates the Eurofisc network for the exchange of information on cross-border fraud, Article 33.

²⁴² Article 10, Regulation 904/2010.

²⁴³ Article 10(2), Regulation 904/2010.

²⁴⁴ Article 11, Regulation 904/2010.

²⁴⁵ Article 55(1), Regulation 904/2010.

²⁴⁶ Article 55(3), Regulation 904/2010.

²⁴⁷ Article 55(5), Regulation 904/2010.

4.1.3. Punitive enforcement in the area of banking law and financial markets

Information may freely circulate among banking supervisors and may even be referred to judicial authorities in case suspicions of an offence emerge. This may result in some cases in the protection of party's procedural rights being lowered or circumvented, in particular if different rules apply, e.g. to the gathering of evidence.²⁴⁸

4.1.3.1. ECB

Under the SSM framework, the ECB and the NCAs are subject to a general obligation to exchange information.²⁴⁹ Moreover, when the ECB exercises its power to request information from supervised entities under Article 10 of the SSM Regulation, it has the duty to make that information available to the NCA of that entity,²⁵⁰ which must be done in a timely and accurate manner.²⁵¹ Also, the results of the ECB investigations may be used as evidence in administrative punitive proceedings at the national level.²⁵² That is the case, for instance, when the ECB considers it necessary to impose a penalty but it does not have a direct competence to do so (e.g., a penalty for a breach of a national requirement, or a penalty attributable to a natural person). In such instances, it may require the NCA to open enforcement proceedings at national level.²⁵³ In this context, there is no specific provision governing the exchange of information from the ECB to the NCAs for the purpose of opening and carrying out national enforcement proceedings. However, considering the general obligation to exchange information, it seems evident that the ECB will share all the relevant information with the NCA, such as information or documents obtained throughout its supervisory work and that led to the suspicion of a breach.

Furthermore, according to the referral mechanism established by Article 136 of the SSM Framework Regulation, when the ECB 'has reason to suspect that a criminal offence may have been committed, it shall request the relevant NCA to refer the matter to the appropriate authorities for investigation and possible criminal prosecution, in accordance with national law'.²⁵⁴ The Regulation did not introduce a direct channel with national

²⁴⁸ C. Eckes, R. D'Ambrosio, 'Composite administrative procedure in the European Union', *ECB Legal Working Paper Series*, no. 20, 2020, pp. 5-6.

²⁴⁹ Article 20 SSM Framework Regulation.

²⁵⁰ Article 10(3) SSM Regulation and Art. 139(3), SSM Framework Regulation.

²⁵¹ Article 21(2) SSM Framework Regulation.

²⁵² Eckes, D'Ambrosio, (no. 238).

²⁵³ Article 18(5) SSM Regulation.

²⁵⁴ Article 136, SSM Framework Regulation.

criminal authorities, but preferred to rely on the mediation of NCAs instead. Some authors have argued that a direct contact with national prosecutors would have made the exchange of information easier and granted a better coordination.²⁵⁵ Again, in this context, there is no specific provision governing the exchange of information from the ECB to the NCAs for the purpose of referring the matter to criminal enforcement authorities. However, considering the general obligation of exchange of information, it seems evident that the ECB will share all the relevant information with the NCA, such as information or documents obtained throughout its supervisory work and that led to the suspicion of a criminal offence. Once the ECB reported to the NCAs, national rules on the transfer of information from the administrative to the criminal authorities apply and it is up to the NCAs to transmit the information gathered to criminal agencies and assure the follow-up of the case. As a result, the information gathered during a Union administrative investigations may be used as evidence in national punitive proceedings. Since Union law does not provide clear rules on the procedural admissibility of evidence collected by Union bodies in national proceedings, the matter continues to be governed by national law.²⁵⁶

On the other hand, national authorities themselves may require the ECB to disclose information acquired during its supervisory tasks for an ongoing investigation.²⁵⁷ To address this issue, in June 2016 the ECB adopted a Decision on the disclosure of confidential information in the context of criminal investigations,²⁵⁸ regulating the conditions for the cooperation between the ECB and the national criminal authorities. Although those conditions are largely determined by national law, EU law has certain implications, stemming from ‘the principle of sincere cooperation, the principles of cooperation in good faith and the obligation to exchange information within the SSM, the obligation to protect personal data and the obligation of professional secrecy’.²⁵⁹

The ECB may also take the final decision based on the information provided to it by NCAs. That is the case when supervisory decisions of the ECB are based on draft decisions or preparatory work prepared by the NCAs, either upon request of the ECB or on the NCA’s own initiative.²⁶⁰ Moreover, the independent Investigating Unit within the ECB is expressly granted access

²⁵⁵ S. Allegrezza, ‘The Single Supervisory Mechanism: Institutional Design, Punitive Powers and the Interplay with Criminal Law’, in: Allegrezza (ed.), (no.142), p. 37.

²⁵⁶ Eckes, D’Ambrosio, (no.238).

²⁵⁷ Allegrezza, (no. 142), p. 40.

²⁵⁸ Decision (EU) 2016/1162 of the European Central Bank of 30 June 2016 on disclosure of confidential information in the context of criminal investigations (ECB/2016/19), OJ L 192, 16.7.2016, pp. 73-76.

²⁵⁹ *Ibid.*, recital 3.

²⁶⁰ Articles 90-91, SSM Framework Regulation.

to all documents and information gathered by the relevant NCAs in the course of their supervisory activities.²⁶¹ In practice this would lead to the sharing of information between NCAs and the ECB for the purpose of investigating a breach for which the ECB can impose punitive sanctions.

4.1.3.2. ESMA

The legal framework for the exchange of information and cooperation between ESMA and national competent authorities is governed by several provisions spread among different sectorial legislation. First, Article 35 of the ESMA Regulation requires competent authorities of Member States to provide ESMA with any necessary information for fulfilling its duties, provided they have legal access to it and the request is justified in relation to the specific duty in question. Vice versa, upon a duly justified request, ESMA may provide information to national authorities, subject to professional secrecy obligations.

Similarly, Article 27 of the CRAR and Article 84 of the EMIR mandate the timely exchange of information between ESMA, competent authorities, and other relevant bodies, including the ECB, when necessary to fulfil their duties. Confidential information shared must strictly be used to carry out these duties.

Furthermore, the Benchmark Regulation insists on the importance of fostering the systematic sharing of relevant information among competent authorities and reinforcing their mutual assistance and cooperative obligations, especially in light of growing cross-border financial activity.²⁶² It further requires the necessity of maintaining strict professional secrecy to ensure the efficiency of information transmission and to uphold the protection of individual rights.²⁶³ In addition, any exchange or transmission of information by ESMA should take place in accordance with the EU Data Protection Regulation.²⁶⁴ Article 38 of the Benchmark Regulation further details the conditions under which a competent authority may disclose information received from another competent authority. Such disclosure is

²⁶¹ Article 125(3), SSM Framework.

²⁶² Recital 60, Benchmark Regulation.

²⁶³ *Ibid.*

²⁶⁴ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, pp. 1-22, later repealed by Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, pp. 39-98.

admitted only if the competent authority providing the information has given its written agreement and the information is disclosed only for the purposes agreed upon or such disclosure is ‘necessary for legal proceedings’.²⁶⁵

Moreover, as part of ESMA’s coordinating role, Article 25 MAR expressly provides for the NCAs’ obligation to cooperate with each other and with ESMA, in particular through the exchange of information, and cooperation in investigations, supervision and enforcement activities. A competent authority may refuse to act on a request for information or a request to cooperate only in exceptional circumstances.²⁶⁶ Interestingly, Article 25 MAR also provides that, in Member States where infringements of the MAR are criminally sanctioned, competent authorities must ensure that NCAs are equipped with all the necessary powers to liaise with judicial authorities within their jurisdiction to receive specific information related to criminal investigations or proceedings concerning those infringements and provide the same to other competent authorities and ESMA.²⁶⁷

4.1.4. Competition law enforcement

Regulation 1/2003 marked a departure from the previous centralised enforcement model of competition law, establishing instead a system based on close cooperation between the European Commission and the competition authorities of the Member States, structured as a network.²⁶⁸ The exchange of information between them, as well as their admissibility and evidential use, is possible under the conditions set out in Article 12 of Regulation 1/2003.²⁶⁹ This provision creates a legal basis for the circulation of information within the network formed by the Commission and the NCAs, while safeguarding

²⁶⁵ Article 38, Benchmark Regulation.

²⁶⁶ Listed in Article 25(2), MAR.

²⁶⁷ Article 25(1), § 4, MAR.

²⁶⁸ ECJ, *France Télécom v. Commission*, 08.03.2007, T-339/04, § 70.

²⁶⁹ Recital 15, ECN+ Directive.

the procedural rights of the undertakings concerned.²⁷⁰ Additional aspects of these cooperation are dealt in the ECN+ Directive.²⁷¹

Article 12 of Regulation 1/2003 deals with the exchange and use of information both vertically (between the EU Commission and NCAs) and horizontally (between different NCAs).²⁷² It empowers the Commission and the competition authorities of the Member States to share with each other, and to rely upon as evidence ‘any matter of fact or of law, including confidential information’.²⁷³ However, information exchanged is strictly limited to use for proving violations of EU competition law and must be confined to the subject-matter for which it was originally collected by the transmitting authority (purpose limitation).²⁷⁴ Furthermore, any information exchanged covered by the obligation of professional secrecy remains protected and cannot be disclosed.²⁷⁵

Conversely, Regulation 1/2003 does not explicitly address the exchange of information or its admissibility as evidence by authorities other than competition authorities.²⁷⁶ The ECJ, however, has generally accepted that the Commission may use evidence transmitted by a national authority other than a competition authority. As regards the exchange of information between national criminal authorities and the Commission, the ECJ held that it was possible for the Commission to use in its proceedings evidence produced by the prosecuting authorities of a Member State in a criminal investigation in

²⁷⁰ However, it shall be mentioned that it has been questioned whether the system introduced by Article 12 of Regulation 1/2003 does respect the defence rights of the undertakings. See, D. Reichelt, ‘To What Extent Does the Co-operation within the European Competition Network Protect the Rights of Undertakings?’, *Common Market Law Review*, 2005, vol. 42, no. 3, 2005-06, p. 745, DOI: 10.54648/COLA2005021; D. Waelbroeck, ‘Twelve Feet All Dangling Down and Six Necks Exceeding Long. The EU Network of Competition Authorities and the European Convention on Fundamental Rights’, in: C.-D. Ehlermann, I. Atanasiu (eds.), *European Competition Law Annual 2002: Constructing the EU Network of Competition Authorities*, Oxford, United Kingdom, Hart, 2004; M. Kozak, ‘ECN+ Directive: A Missed Opportunity for Strengthening the Rights of Parties?’, in: C. S. Rusu, A. Looijestijn-Clearie, M. Veenbrink & S. Tans (eds.), *New Directions in Competition Law Enforcement*, Radboud Economic Law Series, vol. 4, WLP, The Netherlands, 2020.

²⁷¹ Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, OJ L 11, 14.1.2019, pp. 3–33. In particular, Chapter VII on mutual assistance.

²⁷² M. Luchtman, A. Karagianni and K. Bovend'Eerd, ‘EU administrative investigations and the use of their results as evidence in national punitive proceedings’, in: F. Giuffrida, K. Ligeti (eds.), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, Report, University of Luxembourg, 2019.

²⁷³ Article 12(1), Regulation 1/2003.

²⁷⁴ Article 12(2), Regulation 1/2003.

²⁷⁵ Article 28(2), Regulation 1/2003.

²⁷⁶ M. Luchtman, A. Karagianni and K. Bovend'Eerd, ‘EU administrative investigations and the use of their results as evidence in national punitive proceedings’, (268).

application of national criminal law.²⁷⁷ Accordingly, the ECJ held that Article 12 of Regulation 1/2003 does not prevent the Commission from relying on evidence transmitted by a national authority ‘other than a competition authority’.²⁷⁸ In the *FSL* case, the applicants contented that the General Court erred in ruling that the use of evidence transmitted to the Commission by the Italian Guardia di Finanza (finance police) in the course of a national tax investigation was unlawful. They argued that this evidence was gathered in a national procedure whose objectives differed from those of the procedure before the Commission. However, the ECJ clarified that ‘the lawfulness of the transmission to the Commission by a prosecutor or the authorities competent in competition matters of information obtained in application of national criminal law is a question governed by national law’,²⁷⁹ over which it has no jurisdiction.²⁸⁰ Moreover, the ECJ reasoned that restricting the Commission’s ability to use evidence transmitted by national authorities that are not competition authorities, solely on the basis that such evidence were collected in procedures with different purposes, would ‘excessively hamper the role of the Commission in its task of supervising the proper application of EU competition law’.²⁸¹

4.1.5. GDPR enforcement

The GDPR provides for a specific legal basis for cooperation among DPAs established in different Member States,²⁸² but lacks details about how this cooperation should work, which is largely left to the individual Member States.

An obligation to exchange information stems from the so-called ‘one-stop-shop’ mechanism for enforcement in cases where the alleged infringement took place in a cross-border context. In such instances, the lead supervisory authority is required to enter into dialogue with the other DPAs, exchanging all relevant information with each other, in order to reach consensus on the outcome of the case. Moreover, the GDPR states that DPAs must provide each other with relevant information and mutual assistance.²⁸³ This includes information requests and requests to carry out inspections and investigations on behalf of the DPA of another Member State.²⁸⁴ Requests for assistance cannot in principle be refused, unless the DPA is not competent for

²⁷⁷ ECJ, *Dalmine SpA v. Commission*, 25.01.2007, C-407/04 P.

²⁷⁸ ECJ, *FSL and Others v. Commission*, 27.04.2017, C-469/15 P.

²⁷⁹ *Ibid.*, § 32.

²⁸⁰ *Ibid.*

²⁸¹ *Ibid.*, §§ 35-36.

²⁸² Chapter 7, Section 1, GDPR.

²⁸³ Article 61(1), GDPR.

²⁸⁴ *Ibid.*

the subject-matter of the request or compliance with the request would infringe EU or national law.²⁸⁵ Finally, the GDPR provides for the possibility to carry out joint investigations.²⁸⁶ In addition to relevant provisions of the GDPR, national procedural rules apply for any matter that is not regulated by the GDPR.

Interestingly, the ECJ has intervened on the issue of collaboration between DPAs and other national authorities,²⁸⁷ ruling that it may be necessary for national competition authorities ‘also to examine whether that undertaking’s conduct complies with rules other than those relating to competition law’, such as the GDPR.²⁸⁸ The judgment highlighted that although ‘neither the GDPR nor any other instrument of EU law provides for specific rules in that regard’, the fact remains that ‘the various national authorities are all bound by the duty of sincere cooperation enshrined in Article 4(3) TEU’.²⁸⁹ As such, national administrative authorities ‘must assist each other, in full mutual respect, in carrying out their tasks’ and ‘refrain from any measure which could jeopardise the attainment of the European Union’s objectives’.²⁹⁰

In parallel, the European Commission has put forward a proposal for a GDPR Procedural Regulation to ‘streamline cooperation between DPAs when enforcing the GDPR in cross-border cases’.²⁹¹ Although limited to the relationship between DPAs, a proposed amendment by the LIBE committee of the European Parliament seeks to extend its scope. This proposal mandates that DPAs ‘strive to communicate the information obtained to national and Union supervisory authorities competent in data protection and other areas, including competition, financial services, energy, telecommunications and consumer protection authorities, where the information is deemed relevant to the tasks and duties of those authorities’.²⁹² Yet the amendment continues to leave DPAs wide discretion, since they may disclose the information solely if they regard it as relevant.

²⁸⁵ Article 61(4), GDPR.

²⁸⁶ Article 62(1), GDPR.

²⁸⁷ Spark Legal and Policy Consulting, ‘GPD R Collaboration between DPAs and other authorities’, 2025, online [https://www.sparklegalpolicy.eu/news/gdpr-collaboration-between-dpas-and-other-authorities-2/#:~:text=The%20judgment%20highlights%20that%20both,considering%20GDPR%20compliance%20\(2\).](https://www.sparklegalpolicy.eu/news/gdpr-collaboration-between-dpas-and-other-authorities-2/#:~:text=The%20judgment%20highlights%20that%20both,considering%20GDPR%20compliance%20(2).)

²⁸⁸ ECJ, *Meta Platforms Inc and Others v. Bundeskartellamt*, 04.07.2023, C-252/21, § 48.

²⁸⁹ *Ibid.*, § 53.

²⁹⁰ *Ibid.*

²⁹¹ European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679’, Communication, COM(2023) 348 final, European Union, 2023.

²⁹² Committee on Civil Liberties, Justice and Home Affairs, *Amendments 219-454*, 2023/0202(COD), European Parliament, 2023, amendment 311.

4.2. Admissibility of data collected from online service providers as evidence

In the absence of specific EU rules on admissibility of evidence, the matter is still largely governed by national law.²⁹³

An exception can be traced in Article 12 of Regulation 1/2003, already mentioned above regarding the transfer of information between the Commission and national competition authorities, and related case-law of the ECJ (see 4.1.4). As noted, Article 12 introduced a ‘hard and fast rule’ of mutual admissibility of evidence, regardless of the differences between legal systems.²⁹⁴ In addition, Article 12(3) of Regulation 1/2003 sets out conditions under which exchanged information can be ‘used as evidence to impose sanctions on natural persons’. Specifically, it allows such use only insofar the law of the transmitting authority foresees sanctions of a similar kind or, in the absence thereof, the information has been collected ‘in a way which respects the same level of protection of the rights of defence of natural persons as provided for under the national rules of the receiving authority’.²⁹⁵ However, in the latter case, information exchanged cannot be used to impose custodial sanctions.²⁹⁶

Despite the lack of specific EU law governing the admissibility of evidence, the ECJ has been called upon to deal with evidentiary issues on a number of occasions.

The ECJ has held that the prevailing principle in EU law is that of ‘unfettered evaluation of evidence’, which entails that the admissibility of lawfully obtained evidence cannot be contested before EU Courts.²⁹⁷ Given the lack of EU level legislation, ‘any type of evidence admissible under the procedural law of the Member States in similar proceedings is in principle admissible’.²⁹⁸ Conversely, the mere fact that evidence may be inadmissible in one Member State is not enough to consider that it is inadmissible under EU law.²⁹⁹ The ECJ has also affirmed that there is no provision in EU law that expressly prohibits evidence obtained unlawfully, for example in breach of fundamental rights, from being taken into account in judicial proceedings, and, in general terms, ‘[t]here is no provision that expressly prohibits evidence obtained unlawfully, for example in breach of fundamental rights,

²⁹³ See, National Reports and Comparative Chapter.

²⁹⁴ M. Luchtman, A. Karagianni and K. Bovend’Eerdt, ‘EU administrative investigations and the use of their results as evidence in national punitive proceedings’, (no. 268).

²⁹⁵ Article 12(3), Regulation 1/2003

²⁹⁶ *Ibid.*

²⁹⁷ ECJ, *Siemens v. Commission*, 19.12.2013, C-239/11 P, C-489/11 P and C-498/11 P, § 128.

²⁹⁸ ECJ, *Goldfish and Others v. Commission*, 08.09.2016, T-54/14, § 43; ECJ, *Met-Trans and Sagpol*, 23.03.2000, C-310/98 and C-406/98, § 29.

²⁹⁹ ECJ, *Goldfish and Others v. Commission*, (no. 283), §§ 78-79.

from being taken into account.³⁰⁰ However, this does not mean that any information can be admissible as evidence, regardless of how it has been obtained, without taking into account fundamental rights and the general principles of EU law. Indeed, it is also well established in the case-law of the ECJ that respect for fundamental rights is a prerequisite for the legality of EU acts, and any measures that are incompatible with those rights are deemed unacceptable within the EU.³⁰¹ As a result, the Court has affirmed that EU law does not accept the use of evidence that has been obtained ‘in complete disregard of the procedure laid down for gathering it and designed to protect the fundamental rights of interested persons’.³⁰² The application of that procedure should, therefore, be regarded as an ‘essential procedural requirement’ within the meaning of Article 263(2) TFEU, without the need to prove that non-compliance with that procedure has resulted in harm to the person relying on it.³⁰³ Therefore, the fact that the Commission is bound to respect the general principles of EU law, including fundamental rights, implies that evidence that has been collected or processed in contravention of fundamental rights should, in principle, be considered inadmissible.³⁰⁴ Accordingly, the Court has ruled that if an inspection decision is annulled or procedural irregularities are identified during the investigation, the Commission is barred from relying on any documents or evidence obtained through that investigation in subsequent infringement proceedings.³⁰⁵ Nevertheless, the ECJ have admitted that, in certain instances, unlawful evidence may be deemed admissible in punitive proceedings, even when it is inculpatory for the suspect or the person concerned.³⁰⁶

In this context, the judgement in *Goldfish BV v Commission* offers an occasion to reflect about the balance made by the ECJ between effectiveness

³⁰⁰ ECJ, *Franchet and Byk v. Commission*, 08.07.2008, T-48/05, § 75.

³⁰¹ See, ECJ, *Kadi and Al Barakaat International Foundation v. Council and Commission*, 03.09.2008, C-402/05 P and C-415/05 P, § 284 and the case-law cited; ECJ, *Almamet v. Commission*, 12.12.2009, T-410/09, not published, § 39 and the case-law cited.

³⁰² ECJ, *Goldfish and Others v. Commission*, (no. 283), § 46.

³⁰³ See, to that effect, ECJ, *Commission v. ICI*, 06.04.2000, C-286/95 P, §§ 42 and 52; ECJ, *Almamet v. Commission*, (no. 286), § 39 and the case-law cited.

³⁰⁴ F. Castillo de la Torre, E. Gippini Fournier, *Evidence, proof and judicial review in EU Competition Law*, Cheltenham, United Kingdom, Edward Elgar Publishing Limited, 2nd ed., 2024.

³⁰⁵ ECJ, *Roquette Frères v. Directeur général de la concurrence, de la consommation et de la répression des fraudes*, 22.10.2002, C-94/00, § 49; ECJ, *Deutsche Bahn and Others v. Commission*, 18.06.2015, C-583/13 P, § 45; ECJ, *Les Mousquetaires and ITM Entreprises v. Commission*, 09.03.2023, C-682/20 P, § 125.

³⁰⁶ J. Vervaele, ‘Lawful and Fair Use of Criminal Evidence in the EU: The Unwritten Script for European Enforcement Agencies’, in: Luchtman, Ligeti, Vervaele (eds.), (no. 52).

of EU investigations and the protection of fundamental rights.³⁰⁷ Specifically, the case addressed the lawfulness of using recordings of telephone conversations, made in secret by private third parties in violation of the right to private life, as evidence of a competition law infringement. The General Court considered that the Commission was fully entitled to use them as evidence. In doing so, the Court based its reasoning on three key considerations, namely the respect of the procedure laid down for inspection, the fact that the undertaking under investigation was given the opportunity to exercise its defence rights, and that the contested recordings were not the sole evidence of the infringement.³⁰⁸ This might, however, raise some concerns as the Court concluded that information gathered in violation of the right to private life protected by Article 7 of the Charter might still be relied upon by the Commission to impose sanctions, insofar as the violation was not committed by the EU authority itself.

The ECJ has equally rendered several judgements on the transfer and subsequent use of evidence between different proceedings in the area of VAT enforcement.

In the *WebMindLicenses* case, the ECJ provided clear instructions on the exclusion of evidence in an administrative procedure when the standards of the rights of defence and an effective judicial remedy are not met.³⁰⁹ The ECJ affirmed that the transfer of evidence from a parallel criminal procedure to a tax procedure is not precluded as such under EU law, as long as the gathering of such evidence during the criminal investigation and its subsequent use in the administrative context do not infringe the rights safeguarded by EU law. Specifically, the ECJ considered that as far as VAT procedures are concerned, EU law, including the fundamental rights guaranteed in the EU legal order, does apply.³¹⁰ A further key point established by the ECJ concerns the admissibility of evidence obtained through investigative measures conducted without prior judicial authorisation; such evidence is not automatically inadmissible, if sufficient safeguards exist to protect the rights of individuals against any abuse and arbitrariness. Moreover, the ECJ emphasised the critical importance of the right to an effective judicial remedy, underscoring that, in order for judicial review to be effective, courts reviewing decisions implementing EU law must

³⁰⁷ M. Simonato, 'Illicit but admissible evidence', *EU Law Enforcement blog*, 2016, online <https://eulawenforcement.com/?p=98#>.

³⁰⁸ ECJ, *Goldfish and Others v. Commission*, (no. 283).

³⁰⁹ Vervaele, (no. 291); M. Richardson, 'Unlawfully Obtained Evidence: Follow the Court of Justice of the European Union if You Please', *EC Tax Review*, 2021, vol. 30, no. 5-6, DOI: 10.54648/ECTA2021027.

³¹⁰ ECJ, *Åkerberg Fransson*, 26.02.2013, C-617/10, § 19.

be able to verify whether the evidence underpinning that decisions was obtained and used in breach of rights guaranteed by EU law.

In *Glencore*,³¹¹ the ECJ extended the principle elaborated in *WebMindLicenses* affirming that first, the parallel proceedings do not need to be against the same person, and second, the parallel proceedings may be administrative rather than criminal. In the case at hand, the Hungarian tax authority based its decisions on evidence obtained by the same authority in a separate administrative proceeding concerning Glencore's suppliers (a different taxpayer). However, the tax authorities are required to observe the rights guaranteed under EU law, including the rights of the defence, especially the right to be heard and of access to the file.

The ECJ set out three key conditions under which administrative authorities can base their decisions on evidence from other proceedings in order to protect the fundamental rights of the parties. First, administrative authorities must maintain some leeway when considering relevant materials from other proceedings. Second, the taxable person must be able to have access to that evidence and to any other documents which may be helpful in the exercise of the rights of the defence. Finally, there must be an adequate judicial review of the collection and use of such evidence.

These conditions are relevant not only in VAT cases, but also with regard to any administrative proceedings that implement EU law. Accordingly, there can be little doubt that these principles extend to proceedings involving the use of evidence obtained from OSPs.

5. CONCLUSION

As the analysis reveals, the current EU legal framework provides only limited and fragmented possibilities for EU authorities to directly request data from OSPs.

Overall, the EU legislation applicable to the administrative proceedings of the DG COMP, the ECB and ESMA entrusts the latter with far-reaching investigatory powers in their respective areas of enforcement. Yet, neither DG COMP nor the ECB are expressly provided with a legal basis to request data from OSPs. While DG COMP and the ECB are both equipped with a general

³¹¹ While *WebMindLicenses* concerned the situation of a tax authority voluntarily choosing to rely on evidence gathered in the context of still pending criminal proceedings, *Glencore* concerned a different situation where a national law required the tax authority to follow the previous legal findings which it had reached in its own previous administrative proceedings. See M. Szydło, 'How far can previous rulings or evidence determine an individual administrative decision? *Glencore's* implications for decisions within the scope of EU law', *Common Market Law Review*, vol. 58, no. 2, 2021, pp. 505–528, DOI: 10.54648/COLA2021027.

ECJ, *Glencore Agriculture Hungary Kft.*, (no. 188).

power to request information under Regulation 1/2003 and the SSM Regulation, respectively, these powers differ significantly in scope. Under Article 10 SSM Regulation, such requests are narrowly confined to supervised credit institutions and their service providers, thereby excluding OSPs under a literal interpretation. In contrast, Article 18 of Regulation 1/2003 is framed in broader terms, in principle enabling DG COMP to address requests to any private third party, including OSPs. Such interpretation, however, raises concerns regarding the sufficiency of procedural safeguards, particularly in light of the absence of prior judicial authorisation to issue a decision to request for information, the concentration of investigatory and sanctioning powers in the hands of DG COMP, and the deferred activation of defence rights until the statement of objections is issued, especially when intrusive data access is involved. While the ECJ has upheld the compatibility of such proceedings with Article 6 of the ECHR, provided that *ex post* judicial review is available, doubts remain concerning compatibility with Article 7 of the Charter. In this context, the ECJ's case law emphasises that any interference with the right to privacy and data protection must be subject to strict scrutiny, be limited to what is strictly necessary to achieve the legitimate objective pursued and be accompanied by adequate and effective safeguards. In particular, the Court has distinguished between 'serious' and 'non-serious' interferences, the former requiring prior judicial authorisation.

As regards administrative proceedings within the SSM, the legal obstacles to accessing data directly from OSPs are even more evident, in light of the narrow legal basis to request information, as well as the adequacy of procedural safeguards afforded. In particular, the legal framework governing the SSM appears problematic to the extent that it does not guarantee the unlimited judicial review by the ECJ.

Conversely, the sectorial legislation governing the enforcement powers of ESMA explicitly provides for the possibility to request 'records of telephone and data traffic', albeit subject to some limitations. While some legal provisions are drafted in broad terms that could, in principle, allow for an extensive interpretation, this approach has not been adopted in practice. In any event, any such interpretation must comply with general principles, particularly the requirements of necessity and proportionality. More broadly, several EU regulations in the field of financial markets grant NCAs in the Member States the power to require, insofar as permitted by national law, existing data traffic records 'held by a telecommunications operator'. The financial markets sector thus represents a prominent example where EU law acknowledges the evidentiary relevance of electronic data held by telecommunications providers and provides a specific legal basis for its acquisition (e.g., Article 23(2)(h) MAR). However, the exercise of such

powers is generally contingent upon prior judicial authorisation and is restricted to investigations concerning certain serious forms of misconduct.

Overall, the current EU framework provides a patchwork of provisions that, while offering potential avenues for requesting data from OSPs in administrative punitive proceedings, fall short of delivering a coherent approach. The presence of general legal bases might be interpreted extensively to include OSPs, but such interpretations are not exempted from risk of breach to fundamental rights of persons involved. Conversely, in sectors such as financial regulation, where the need for such data has been recognised, the EU has introduced more tailored provisions that appropriately regulate access to data.

In conclusion, while EU law does not preclude the possibility of requesting data from OSPs in the context of administrative enforcement, it imposes the respect of strict procedural safeguards. These include not only the presence of a clear legal basis, but also compliance with principles of necessity, proportionality, and purpose limitation, along with effective judicial oversight and the protection of defence rights. Future legislative developments should aim to harmonise these requirements across enforcement domains and provide clearer guidance on when and how evidence from OSPs may be lawfully accessed and used.

3. GATHERING OF ELECTRONIC EVIDENCE FOR THE PROTECTION OF THE FINANCIAL INTERESTS OF THE EU

M. SICLARI and J. A. E. VERVAELE

1. THE EUROPEAN ANTI-FRAUD OFFICE (OLAF)

The protection of the financial interests of the European Union (EU) has become increasingly critical, as the need to safeguard EU funds from illegal exploitation and ensure their efficient and lawful use remains central to achieving the Union's policy objectives.

Set up in 1999 in response to the events that led to the resignation of the Santer Commission, the European Anti-Fraud Office (OLAF) is the first body of the Union established to address misconduct affecting the EU budget. Through its administrative investigations, OLAF plays a crucial role in detecting and combatting irregularities, fraud, corruption, and other illegal activities affecting the Union budget. However, the increasing reliance on data in today's financial investigations raises significant concerns, requiring a clearly defined legal framework. These concerns are not absent in the context of OLAF's investigations, as demonstrated by criminal proceedings against its former Director-General, who was convicted by Belgian judicial authorities and handed a one-year suspended prison sentence for the unlawful interception of a telephone conversation during an OLAF investigation.¹

This chapter analyses OLAF's legal framework, focusing on the scope and limits of its investigative powers in the digital realm. In particular, it explores OLAF's authority to gather electronic evidence from third-party private actors, such as Online Services Providers (OSPs), in its administrative investigations, as well as on the rules governing the transfer and admissibility of such evidence in follow-up proceedings. The chapter is solely based on the EU-level legal framework, whose centerpiece is now represented by

¹ L'Echo, La peine de l'ex-patron de l'OLAF Giovanni Kessler Réduite en appel, 2019, online <https://www.lecho.be/economie-politique/belgique/general/la-peine-de-l-ex-patron-de-l-olaf-giovanni-kessler-reduite-en-appel/10552111.html>.

Regulation 883/2013,² as last amended by Regulation 2020/2223³ (hereinafter ‘OLAF Regulation’).

OLAF is charged with a range of duties set out in Article 1 of the OLAF Regulation, with its primary mission being to conduct administrative investigations into irregularities affecting the financial interests of the Union, both internally, meaning within the EU’s institutions, bodies, offices and agencies, and externally, investigating the conduct of persons or economic operators both within the territory of Member States and in third countries. Beyond its proper autonomous investigations (both external and internal), OLAF can assist the competent authorities of Member States (i.e. coordination activities),⁴ and support⁵ or complement investigations of the EPPO.⁶

OLAF has no legal personality of its own. Whilst being a service of the European Commission, it enjoys fully financial and functional independence, allowing it to conduct its investigations in complete independence. In this context, OLAF is headed by a Director-General, who is appointed by the Commission according to a special procedure designed to ensure OLAF’s independence from the Member States and EU institutions, including the Commission itself.⁷ To further reinforce that independence, a Supervisory Committee, composed of external independent experts highly qualified in OLAF areas of activity, has been established to monitor the implementation of its investigative function.⁸

As regards OLAF’s autonomous investigations, its investigative powers stem from different legal instruments, giving rise to a complex legal framework. As mentioned, the OLAF Regulation defines the Office’s mandate, powers and procedures to be followed. Yet, this general legal framework is complemented by an array of different pieces of legislation, such as Regulation 2988/95 on the protection of the European Communities financial interests,⁹ Regulation 2185/96 concerning on-the-spot checks and

² Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ L 248, 18.9.2013, pp. 1-22.

³ Regulation (EU, Euratom) 2020/2223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor’s Office and the effectiveness of the European Anti-Fraud Office investigations, OJ L 437, 28.12.2020, pp. 49-73.

⁴ Article 12b OLAF Regulation.

⁵ Article 12e OLAF Regulation.

⁶ Article 12f OLAF Regulation.

⁷ Article 17 OLAF Regulation.

⁸ Article 15 OLAF Regulation.

⁹ Council Regulation (EC, Euratom) No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests, OJ L 312, 23.12.1995, pp. 1-4.

inspections,¹⁰ and numerous references to national law, as well as sectorial EU legislation. In addition, OLAF's activities shall be carried out in accordance with its internal rules of procedure, specifically the 2016 Guidelines on Digital Forensic Procedures for OLAF Staff and the 2021 Guidelines on Investigation Procedures for OLAF Staff and on Data Protection for Investigative Activities.

Despite its primary task to conduct administrative investigations, OLAF lacks any prosecutorial or coercive powers. Unlike DG COMP, the ECB or ESMA,¹¹ OLAF cannot impose (punitive) administrative sanctions on its own nor is allowed to use force. As OLAF is not a judicial authority, it cannot conduct judicial investigations and neither can it initiate prosecutions, in case a criminal conduct is found.¹² At the end of the investigation, the Office can merely draw up a final report, which may be accompanied by recommendations as to the disciplinary, administrative, financial or judicial actions to be taken by the relevant EU institutions, bodies, offices, and agencies, or by the competent authorities of the Member States concerned.¹³ While authorities of the Member States share with the Union binding enforcement responsibilities to protect the EU financial interests under Article 325 Treaty on the Functioning of the EU (TFEU),¹⁴ OLAF final reports and their accompanying recommendations have been considered to lack binding legal effect. Such interpretation stems from provisions of the OLAF Regulation, which leave it to the discretion of the authorities to whom the reports are addressed to decide whether to take action or not.¹⁵ National authorities only have a duty to examine the forwarded information but remain free to assess that information. As a result, these reports have, until now, been regarded as merely preparatory measures, as they do not bring about a distinct change in the legal position of the persons concerned. Accordingly, the Court

¹⁰ Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities, OJ L 292, 15.11.1996, pp. 2-5.

¹¹ See M. Siclari, S. Tosza, European Union, in this volume; M. Luchtman, J. Vervaele (eds.), *Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with other EU law enforcement authorities (ECN/ESMA/ECB)*, Report, European Commission, OLAF, 2017.

¹² A. Met-Domestici, 'The Hybrid Architecture of the EPPO, From the Commission's proposal to the Final Act', *eu crim*, no. 3/2017, pp. 143–149.

¹³ Article 11 OLAF Regulation.

¹⁴ As reaffirmed by the Court of Justice of the European Union (ECJ) in landmark *Greek Maize* (ECJ, *Commission v. Greece*, 21.09.1989, C-68/88) and *Taricco* (ECJ, *Taricco and Others*, 08.09.2015, C-105/14) cases.

¹⁵ Article 11 OLAF Regulation merely provides for the forwarding of information to national judicial authorities, which remain free, in the context of their own powers, to assess the content and significance of that information and, thus, the action to be taken if necessary.

og Justice of the EU (ECJ) has consistently declared actions for annulment of OLAF's investigative acts and final reports inadmissible.¹⁶

However, amendments introduced by Regulation 2020/2223 have sought to improve the effectiveness of the follow-up to OLAF recommendations, notably introducing the possibility for OLAF to request national competent authorities to inform the Office on the reasons for non-implementation.¹⁷ Evidence collected during OLAF investigations is therefore highly likely to end up before a different EU or national authority, whether administrative or criminal, thus raising important questions regarding their admissibility in such proceedings.¹⁸

2. PUNITIVE ADMINISTRATIVE PROCEEDINGS: GENERAL LEGAL FRAMEWORK

Before delving into the specifics of the OLAF's legal framework, it is important to note that the general principles of EU law and fundamental rights that govern the Union's action also apply to OLAF settings. As a result, OLAF is required to conduct its investigations in accordance with the provisions of EU primary law, ensuring respect for fundamental rights and adherence to procedural guarantees.¹⁹

The obligation to respect fundamental rights in the context of OLAF investigations initially stemmed from the case law of the ECJ, which, in the absence of explicit provisions in OLAF's founding Regulation, progressively deduced procedural guarantees from EU primary law. The legal framework has since evolved, with the current OLAF Regulation codifying several provisions that now explicitly require the Office to conduct its investigation in adherence with key fundamental rights and procedural guarantees. Even when not explicitly mentioned, OLAF remains bound to respect fundamental rights and comply with the principles recognised in the Charter of Fundamental Rights of the EU.²⁰

¹⁶ ECJ, *Gómez-Reino v. Commission*, 18.12.2003, T-215/02; *Comunidad Autónoma de Andalucía v. Commission*, 13.07.2004, T-29/03; *Tillack v. Commission*, 4.10.2006, T-193/04; K. Bovend'Eerd, *The Protection of Fundamental Rights in OLAF Composite Enforcement Procedures*, New York, United States of America, Springer, 2024.

¹⁷ Article 11(5), second subparagraph, OLAF Regulation.

¹⁸ F. Giuffrida, G. Theodorakakou, 'The Use of Investigative Results as Evidence in National Punitive Proceedings: The Case of OLAF' in: M. Luchtman, K. Ligeti & J. Vervaele (eds.), *EU Enforcement Authorities: Punitive Law Enforcement in a Composite Legal Order*, pp. 167–194, Oxford: Hart Publishing, 2023.

¹⁹ D. Riochet, N. Mavromati, 'The Protection of Fundamental Rights and Procedural Guarantees in OLAF Investigations: a 25-Year Journey', *Eucrim*, no. 4/2024, pp. 316–323.

²⁰ Recital 51 OLAF Regulation.

Among these, the principle of proportionality in the context of OLAF investigations implies that the measures and actions undertaken by the Office must not exceed what is necessary to achieve the objectives of the investigation. The principle of proportionality is now to be mandatorily considered when deciding to open an investigation,²¹ as regards the means to be deployed, exchange of information as well as the duration of OLAF investigations.²²

Furthermore, the right to good administration, enshrined in Article 41 of the Charter, guarantees that every individual has the right to have their affairs handled impartially, fairly and within a reasonable time by the institutions of the Union. This right encompasses several key elements, including the right to be heard, the right to have access to the file, as well the obligation of the administration to give reasons for its decisions. All these guarantees are therefore applicable to OLAF and must be observed in its investigative activities. The ECJ further reinforced these obligations in *Planistat Europe*, where it held that the right to good administration includes a duty of care on the part of OLAF, which required it to act with care and caution.²³

3. PUNITIVE ADMINISTRATIVE PROCEEDINGS: OLAF'S LEGAL FRAMEWORK

3.1. Requests for data to online service providers

Although various EU-level legal provisions allow OLAF to gather data from private actors in both its internal and external investigations, there is currently no explicit legal basis for OLAF to directly request data from OSPs. In its Opinion 2/2017, the Supervisory Committee of OLAF already acknowledged the absence of rules governing OLAF's competence to 'access or request access to traffic data and electronic communications, including official or private communications stored on devices, media or connected computer systems'.²⁴ Yet, the situation has since evolved, as well exemplified by the recently added possibility for OLAF to inspect privately owned devices used for work purposes.²⁵

²¹ Article 5 OLAF Regulation.

²² Article 7(5) OLAF Regulation.

²³ ECJ, *Planistat Europe and Hervé-Patrick Charlot v. European Commission*, 11.01.2024, C-363/22 P.

²⁴ Opinion No 2/2017 accompanying the Commission Evaluation report on the application of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council (Article 19), (2018/C 404/01), 09.11.2018.

²⁵ Article 3(5) OLAF Regulation.

OLAF might obtain electronic evidence through various alternative ways. This chapter examines the existing possibilities for OLAF to gather data from third-party private actors in its administrative investigations to assess whether, and if so, to what extent, they could be potentially used to request data from OSPs.

Before delving into the specific investigative measures available to OLAF, it should be noted that such measures can only be employed during the course of an OLAF's investigation, meaning at any time between the opening and closing of an investigation. The decision to open an investigation rest with OLAF's Director-General, based on the existence of sufficient suspicion that an illegal activity affecting the financial interests of the Union has taken place,²⁶ also taking into consideration 'the proportionality of the means to be deployed'.²⁷

3.1.1. On-the-spot check and inspections

The gathering of electronic evidence in OLAF investigations could primarily occur within the context of what has been described as 'OLAF's most important power',²⁸ that is on-the-spot checks and inspections. The latter comprises the power to entry premises and to access any relevant information, documents, and data. In this regard, the General Court has ruled that it is for OLAF to decide what is to be considered as 'relevant'.²⁹

Article 5 of Regulation 2185/96 provides that on-the-spot checks and inspections may be carried out not only on 'economic operators concerned' – that is any 'economic operator suspected of having committed, fraud, corruption or any other illegal activity affecting the financial interests of the Union and who is therefore subject to an investigation'³⁰ – but also on 'other economic operators', where strictly necessary to establish whether an irregularity exists.³¹ Undoubtedly, a broad interpretation of the notion of 'other economic operators' could, in principle, include OSPs, thus granting OLAF the power to conduct on-the-spot checks and inspections to access data held by OSPs.

Such interpretation seems to be supported to some extent by the 2016 Guidelines on Digital Forensic Procedures for OLAF Staff.³² Since on-the-

²⁶ Article 5(1) OLAF Regulation.

²⁷ *Ibid.*

²⁸ K. Bovend'Eerdt, 'OLAF'. In: Bovend'Eerdt, (no. 16), p. 111.

²⁹ ECJ, *Vialto Consulting v. Commission*, 26.06.2019, T-617/17, § 68.

³⁰ Article 2 OLAF Regulation.

³¹ Article 5 Regulation 2185/96.

³² OLAF, *Guidelines on Digital Forensic Procedures for OLAF Staff*, 15.02.2016, online https://anti-fraud.ec.europa.eu/document/download/87e5deb1-8a64-42ca-8e08-234355dbe544_en?filename=guidelines_en_bb84583638.pdf.

spot checks and inspections may concern, inter alia, ‘computer data’,³³ a significant portion of OLAF’s on-the-spot checks is in practice often accompanied by digital forensic operations. Notably, Article 7 of the 2016 Guidelines acknowledges the situation where data potentially relevant for the investigation are held by third-party private actors, such as Cloud Service Providers (e.g., Hotmail, Gmail, Yahoo Mail, Dropbox, etc.) or Internet Service Providers, envisaging the possibility for OLAF to request that such data be provided under Article 5 of Regulation 2185/96.

However, guidelines are merely a self-regulatory instrument, laying down internal rules meant to be followed by OLAF staff, without any binding effect.³⁴ In this respect, they lack the status of hard law and thus should only be followed if national law provides for the same powers.³⁵ Therefore, they cannot constitute *per se* a legal basis for OLAF to request data from OSPs. This might explain why this possibility does not seem to have been ever deployed in practice.

Should it be considered a viable option, the rules applicable to such a measure would be those laid down in the OLAF’s legal framework. Following its last amendment, the OLAF Regulation now distinguishes the applicable regime based on whether there is resistance on the part of the economic operator or not. As clarified by the General Court, however, the provisions regarding the potential opposition of the economic operation do not entail the existence of a ‘right to resist’, but merely provide for the consequences in the event of resistance.³⁶ In the absence of resistance, on-the-spot checks and inspections are to be conducted by OLAF solely on the basis of EU law (i.e., OLAF Regulation and Regulation 2185/1996) and national law should be deemed irrelevant.³⁷ That includes the application of the procedural guarantees as clarified in Article 3(8) of OLAF Regulation, which now expressly mention the right not to make self-incriminating statements and the right to be assisted by a person of their choice.³⁸ Furthermore, OLAF conducts on-the-spot checks and inspections upon production of the written authorisation of the Director-General. Such authorisation specifies the subject matter and purpose of the inspection, as well as the legal bases and the corresponding investigative powers stemming from those bases.³⁹ Whenever a written authorisation from the Director-General is required, the

³³ Article 7 Regulation 2185/96.

³⁴ K. Ligeti, *The protection of the procedural rights of persons concerned by OLAF administrative investigations and the admissibility of OLAF Final Reports as criminal evidence*, Report, Directorate General for Internal Policies of the Union, 2017, p. 19.

³⁵ K. Bovend’Eerdt, (no. 16), p. 138.

³⁶ ECJ, *Sigma Orionis SA v. Commission*, 03.05.2018, T-48/16, § 95.

³⁷ *Ibid.*

³⁸ Article 3(5) OLAF Regulation.

³⁹ Article 7(2) OLAF Regulation.

investigative measure undergoes a prior legality check involving the Review Team, which verifies the compliance of the intended investigative measure with legal standards, including its necessity and proportionality, and provide an opinion to the Director-General.⁴⁰

Still, OLAF may come across resistance from the person concerned. Despite the absence of compulsion or subpoena powers, such as the power to impose daily penalty payments, OLAF's investigators can call on national authorities to deploy their coercive powers. In such cases, however, national law does come into play, as the competent authorities of the Member States are required to provide assistance in accordance with the applicable national procedural rules. As a result, if national law requires so,⁴¹ an *ex ante* judicial authorisation must be applied for.⁴²

OLAF has also the power to carry out on-the-spot checks and inspections at the premises of 'economic operators' also in the course of its internal investigations.⁴³ This power is intended to obtain access to 'information relevant to the matter under investigation within the institutions, bodies, offices and agencies'.⁴⁴ In this event, unlike the corresponding provision regarding external investigations,⁴⁵ the Regulation does not restrict the scope of on-the-spot checks and inspections to the economic operator 'concerned', thereby opening up to a possible inclusion of OSPs. While the Regulation does not explicitly stipulate the applicable rules in such a case, it is generally expected that they will adhere to the rules just outlined for external investigations.

To summarise, the potential reliance on the aforementioned legal bases could provide OLAF with the authority to access relevant data held by OSPs. However, the exercise of this power would still require OLAF to entry the premises of an OSP and gather electronic evidence on-site, in compliance with the procedural requirements governing on-the-spot checks and inspections.

⁴⁰ Article 16 Guidelines on Investigation Procedures for OLAF Staff.

⁴¹ Only some Member States provides for *ex ante* judicial authorisation. This is the case, for instance, under French law, while Germany and Italy draw a distinction concerning the cases when such preventive judicial authorisation is required. See M. De Bellis, 'Multi-level Administration, Inspections and Fundamental Rights: Is Judicial Protection Full and Effective?', *German Law Journal*, 2021, vol. 22, no. 3, pp. 416–440, p. 426, DOI: 10.1017/glj.2021.14.

⁴² Article 3(6) OLAF Regulation.

⁴³ Article 4(3) OLAF Regulation.

⁴⁴ *Ibid.*

⁴⁵ Article 3 OLAF Regulation.

3.1.2. Requests for information

The scenario would be different, however, if OLAF were to rely on a general basis of request for information. In this regard, one of the major changes brought by Regulation 2020/2223 is the introduction, in Article 3 of the OLAF Regulation, of an ‘all-encompassing’ duty to cooperate with OLAF during its investigations.⁴⁶ In particular, as part of their duty of cooperation, an economic operator may be obliged to supply relevant information.⁴⁷ Article 3(3) now expressly provides for the power of OLAF to request ‘written and oral information’. This novelty was sought by the Commission in its proposal to amend Regulation 883/2013. Specifically, the proposal intended to further expand the duty to cooperate to include the obligation to answer factual questions and to provide documents,⁴⁸ ‘even if this information may be used to establish against them or against another operator the existence of an illegal activity’.⁴⁹

In this sense, some scholars have argued that such requests should be considered as production orders, enabling OLAF to ‘passively’ obtain information it needs, in addition to its capacity to actively gather information through on-the-spot checks and inspections.⁵⁰ These requests would therefore enable OLAF to request economic operators to supply all the necessary information to OLAF, similarly to what DG COMP already does on the basis of Article 18 of Regulation 1/2003.⁵¹ However, unlike DG COMP, which is entitled to impose periodic penalty payments to compel undertakings to supply information,⁵² OLAF lacks any comparable enforcement mechanism in case of non-cooperation.

It is not clear whether such requests could also be directed towards economic operators which are not under investigations, potentially extending

⁴⁶ K. Bovend'Eerdt, (no. 16).

⁴⁷ K. Bovend'Eerdt, (no. 16).

⁴⁸ The ECJ, in *Orkem* (ECJ, *Orkem v. Commission*, 18.10.1989, C-374/87), has interpreted the right to avoid self-incrimination as being limited to questions that would require the person concerned to admit guilt, thereby distinguishing it from requests for purely factual information. Moreover, this right does not extend to the access and examination of pre-existing documents or records.

⁴⁹ European Commission, *Commission Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 883/2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) as regards cooperation with the European Public Prosecutor's Office and the effectiveness of OLAF investigations*, Proposal, COM/2018/338 final, European Union, 2018, Recital 21.

⁵⁰ K. Bovend'Eerdt, (no. 16), p. 125.

⁵¹ Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (Text with EEA relevance), OJ L 1, 4.1.2003, pp. 1-25.

⁵² See EU Chapter in this book.

their scope to include OSPs. An interpretation of Article 3(3) of the OLAF Regulation in light of the Commission's proposal suggests so. The duty to cooperate, as set out in the Commission's proposal, extended not only to operators directly involved in the investigation but also to any operators who 'might hold relevant information', the only limit being the privilege against self-incrimination, which exempts economic operators from admitting that they have committed an illegal activity.⁵³

Nor it is clear whether the power to request information is confined solely to the context of OLAF's on-the-spot checks and inspections, or if it could be exercised independently from them, as is the case for DG COMP. In this respect, it should be noted that Article 3 of the OLAF Regulation covers 'external investigations' in general, rather than being limited exclusively to on-the-spot checks and inspections, thus leaving some room for a potentially broader interpretation. The interviews conducted, however, do not indicate that such power have been deployed in this manner so far. Rather, the current interpretation seems to favour the more restrictive approach whereby requests for information occur during on-the spot checks.⁵⁴ The standard practice remains that, during such checks, OLAF simultaneously lists categories of documents and materials to which it requires access. Hence, if requests for information are to take place only contextually to on-the spot checks, the exercise of such power over OSPs would require conducting a prior on-the-spot check at the OSP's premises, under the rules and the conditions outlined in Section 3.1.1, which seems an unlikely proposition in the context of investigations concerning entities that have no common interest with the OSP except using the provision of online services.

While a comparable power to request written information exists also in the course of OLAF's internal investigations, its personal scope appears more restricted, being limited to 'officials, other servants, members of institutions or bodies, heads of offices or agencies, or staff members',⁵⁵ thereby excluding OSPs.

3.2. Procedural guarantees

3.2.1. Procedural rights

As regards procedural guarantees applicable to any of the measures described in the previous sections were they applicable to request data from OSPs as third parties, OLAF must respect fundamental rights as laid down in

⁵³ Commission Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 883/2013, (no. 48).

⁵⁴ In this sense Bovend'Eerdt, (no. 16), p. 125 and M. Scholten, M. Simonato, 'EU Report', in: Vervaele and Luchtman (eds.), (no. 11).

⁵⁵ Article 4(2)(b) OLAF Regulation.

Union law, in particular in the Charter. Moreover, persons concerned by OLAF's investigations enjoy the protection of a number of defence rights and procedural safeguards stemming directly from OLAF's legal framework.

Specifically, in the exercise of their powers, OLAF's investigators must act in adherence with the procedural guarantees provided for in Article 9 of the OLAF Regulation. In this respect, in its investigations OLAF shall seek both 'evidence for and against the person concerned'.⁵⁶ Furthermore, investigations shall be conducted 'objectively and impartially and in accordance with the principle of the presumption of innocence'.⁵⁷ Once the investigation is completed, the person concerned shall be given the right to comment on the facts of the case prior to the formulation of any conclusions.⁵⁸ To that end, OLAF must send an invitation containing a summary of the facts and indicating the time limit for submitting comments, which must be no less than 10 days from receipt of the invitation. These comments are to be incorporated into the final investigation report.⁵⁹ Only in exceptional circumstances (i.e., 'in duly justified cases where necessary to preserve the confidentiality of the investigation or an ongoing or future criminal investigation by the EPPO or a national judicial authority'), OLAF's Director-General can decide to postpone the obligation to afford the person concerned the opportunity to submit comments.⁶⁰

While prior to its latest amendment the right to avoid self-incrimination was granted by the OLAF Regulation only to 'any persons interviewed' under Article 9(2), the privilege against self-incrimination is now expressly protected also in the context of on-the-spot checks and inspections.⁶¹ Accordingly, the economic operator concerned shall have the right not to make self-incriminating statements, which should be understood as interpreted by the ECJ in *Orkem*.⁶² In this respect, the material scope of the privilege covers only admissions on part of the person concerned of 'the existence of an infringement', which is incumbent upon the OLAF to prove instead.⁶³

Conversely, the OLAF Regulation contains no explicit provisions regarding the legal professional privilege. Nonetheless, the 2016 Guidelines on Digital Forensic Procedures for OLAF Staff do refer to 'data of a legally privileged nature'.⁶⁴ Should an economic operator claim that a device

⁵⁶ Article 9(1) OLAF Regulation.

⁵⁷ *Ibid.*

⁵⁸ Article 9(4) OLAF Regulation.

⁵⁹ *Ibid.*

⁶⁰ *Ibid.*

⁶¹ Article 3(8) OLAF Regulation.

⁶² Ligeti, (no. 34).

⁶³ ECJ, *Orkem v. Commission*, (no.47), § 35.

⁶⁴ Article 6(3), Guidelines on on Digital Forensic Procedures for OLAF.

contains such data, Article 6(3) of the Guidelines provides that the data must be acquired and placed in a sealed envelope. The representative of the economic operator is then invited to a meeting to resolve the matter before OLAF opens the sealed envelope. In practice, OLAF and the economic operator concerned should reach an agreement on a protocol to be followed. Normally, OLAF's digital-evidence specialists would index the data extracted from the envelope and identify the data in respect of which confidentiality is claimed, in order to exclude them from any subsequent search and ensure that they are not available to OLAF's investigators. Furthermore, in its recent judgement in the *LG and Others v Commission* case, the General Court confirmed the protection of the legal professional privilege in the framework of OLAF's investigations.⁶⁵ In the case at stake, the applicants claimed that the electronic correspondence seized and copied during on-the-spot checks at their premises was protected by the confidentiality of communications between lawyers and their clients. Although the action was dismissed as inadmissible, it nonetheless provided the ECJ an opportunity to address, for the first time, the applicability of the *Akzo Nobel* case law⁶⁶ – where the Court had clarified the scope of legal professional privilege under EU law – to OLAF. In particular, the Court affirmed that, had OLAF issued a final decision rejecting the claim of confidentiality, the applicants would have been entitled to bring an action for annulment under Article 263 TFEU.⁶⁷

For its internal investigations, OLAF must carry out its administrative investigations also subject to the rules on privileges and immunities,⁶⁸ in particular in the case of Members of the European Parliament,⁶⁹ and the existing jurisprudence in this area.⁷⁰

Finally, OLAF must uphold the respect of confidentiality and data protection of information acquired or transmitted in the course of its investigations.⁷¹ In this context, confidentiality of OLAF's investigations has been interpreted by the ECJ as also having the objective of safeguarding the presumption of innocence of persons affected by those investigations, and

⁶⁵ ECJ, *LG and Others v. European Commission*, 20.05.2021, T-482/20.

⁶⁶ ECJ, *Akzo Nobel Chemicals v. Commission*, 17.09.2007, T-125/03 confirmed on appeal by ECJ, *Akzo Nobel Chemicals and Akros Chemicals v. Commission*, 14.09.2010, C-550/07 P.

⁶⁷ ECJ, *LG and Others v. European Commission*, (no. 64), § 61.

⁶⁸ Protocol No 7 on privileges and immunities.

⁶⁹ Chapter III (Articles from 7 to 9), Protocol No 7.

⁷⁰ ECJ, *Willy Rothley and Others v. Parliament*, 26.02.2002, T-17/00, § 73: 'the risk cannot be excluded a priori that, in conducting an investigation, the Office might perform an act prejudicial to the immunity enjoyed by every Member of the Parliament. However, if that were to occur, any Member of the Parliament faced with such an act could, if he considered it damaging to him, avail himself of the judicial protection and the legal remedies provided for by the Treaty'.

⁷¹ Article 10 OLAF Regulation.

therefore their reputation.⁷² Moreover, OLAF is required to comply with Regulation 2018/1725 on the protection of natural persons in relation to the processing of personal data by EU institutions and bodies.⁷³ Accordingly, OLAF has designated a Data Protection Officer (DPO) responsible for the processing of data within the Office.⁷⁴

3.2.2. Remedies

As regards the remedies available against OLAF's investigative measures, the OLAF Regulation does not contain any specific provisions on the judicial review of OLAF's action. Nevertheless, since OLAF's acts are acts of an EU body, they are attributable to the EU legal order and, as such, fall under the exclusive jurisdiction of the ECJ. Yet, the possibility to submit OLAF investigative acts to judicial control through an action for annulment before the ECJ under Article 263 TFEU has long been denied.⁷⁵ The ECJ consistently considered that 'only measures with binding legal effects and capable of affecting the interests of the applicant, by bringing about a distinct change in his legal position, are acts or decisions which may be the subject of an action for annulment'.⁷⁶ In light of this strict interpretation of the admissibility conditions of an action for annulment before the ECJ, actions introduced against OLAF's investigative acts (including final reports) have constantly been declared inadmissible.⁷⁷ Such interpretation has been criticised for creating a considerable hurdle for persons willing to challenge their validity before EU courts.⁷⁸

⁷² ECJ, *Giraudy v. Commission*, 2.05.2007, F-23/05, § 161.

⁷³ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98.

⁷⁴ Article 10(4) OLAF Regulation and Article 43 of Regulation 2018/1725.

⁷⁵ F. Coman-Kund, *Legal Protection against Fundamental Rights Breaches through Factual Conduct by the European Union*, forthcoming.

⁷⁶ ECJ, *IBM v. Commission*, 11.11.1981, C-60/81, § 9.

⁷⁷ ECJ, *Gomez-Reino v. Commission*, (no. 16); ECJ, *Comunidad Autonoma de Andalucia*, (no. 16).

⁷⁸ M. Rodopoulos, K. Pantazatou, 'Judicial Protection Against OLAF's Acts: In search of Effectiveness', *Hellenic Review of European Law*, International Edition, 2013, pp. 133-152; X. Groussot, Z. Popov, 'What's Wrong With OLAF? Accountability, Due Process and Criminal Justice in European Anti-Fraud Policy', *Common Market Law Review*, vol. 47, no. 605-643, 2010.

Neither those acts would be directly challengeable before national courts, since the latter do not have the power to annul EU acts.⁷⁹ Still, during national proceedings based on OLAF investigative acts, a question as to the validity of those acts may arise.⁸⁰ In this case, the person concerned would have the possibility to request the national court to refer a question to the ECJ for a preliminary ruling on the validity of the OLAF's investigative act.⁸¹ However, this option would not be available to a third-party economic operator, such as an OSP, as it is not a party to the national proceedings.

The reasoning of the ECJ rests on the assumption that OLAF's acts are merely preparatory, as national judicial authorities remains free to assess the content and significance of information transmitted and the action to be taken.⁸² Yet, the amendments brought by Regulation 2020/2223 to Article 11 of the OLAF Regulation (corresponding to Article 10 of the previous Regulation 1073/99), as we will see, seems to have introduced a 'mandatory inclusion rule',⁸³ requiring national authorities to consider evidence collected by OLAF as admissible in punitive administrative proceedings irrespective of national evidentiary rules.⁸⁴ Although this *de iure* admissibility of evidence does not affect the discretionary assessment of evidence by national authorities, it results in the automatic inclusion in the national proceeding or case file of evidence despite the fact that it may have been collected in violation of procedural safeguards or fundamental rights, without any possibility to challenge their validity beforehand. Hence, the question arises whether postponing the judicial review of OLAF investigative measures until

⁷⁹ On the difference between direct and indirect judicial review see J. Inghelram, 'Judicial review of investigative acts of the European Anti-Fraud Office (OLAF): A search for a balance', *Common Market Law Review*, vol. 49, 2012, pp. 601–628.

⁸⁰ *Ibid.*

⁸¹ Article 267 TFEU as interpreted by ECJ, *Foto-Frost v. Hauptzollamt Lübeck-Ost*, 22.10.1987, C-314/85.

⁸² ECJ, *Tillack v. Commission*, 04.10.2006, T-193/04: "Article 10(2) of Regulation No 1073/1999 merely provides for the forwarding of information to national judicial authorities, which remain free, in the context of their own powers, to assess the content and significance of that information and, thus, the action to be taken if necessary".

⁸³ J. Vervaele, 'Lawful and Fair Use of Criminal Evidence in the EU: The Unwritten Script for European Enforcement Agencies', in: Luchtman, Ligeti and Vervaele (eds.), (no. 18); J. Vervaele, 'Lawful and Fair Use of Evidence from a European Human Rights Perspective' in F. Giuffrida and K. Ligeti (eds.), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, University of Luxembourg, 2019.

⁸⁴ F. Giuffrida, G. Theodorakakou, 'The Use of Investigative Results as Evidence in National Punitive Proceedings: The Case of OLAF', in: Luchtman, Ligeti and Vervaele (eds.), (no. 18).

the national final decision (if any) based on those investigative measures is compatible with Article 47 of the Charter.⁸⁵

Seemingly demonstrating the openness to consider that problem, the General Court has recently stated, for the first time, that an act of OLAF could be challenged before the ECJ pursuant to Article 263 TFEU.⁸⁶ In the present case, the applicants brought an action seeking for the annulment of an email sent by OLAF, arguing that that email amounted to a ‘tacit decision’ by OLAF rejecting their claim for legal professional privilege. Although the Court dismissed the action as inadmissible, since the email did not contain a definitive position adopted by OLAF, it nonetheless affirmed that, were OLAF to adopt such a decision, the applicants would be entitled to bring action for annulment under Article 263 TFEU.⁸⁷ However, while this interpretation certainly applies to the person under investigation, it remains doubtful whether it would extend to third party economic operators, such as OSPs, allowing them to access this form of redress.

A different way for a person concerned to obtain judicial protection against OLAF’s acts would be introducing an action seeking for compensation of damages under Article 268 TFEU. The latter provision allows claims for damages arising from unlawful actions by EU institutions, including OLAF, provided that certain conditions are met. In such case, the burden of proof rests with the plaintiff. The applicant – whether the person concerned by the investigation or the OSP – must demonstrate a sufficiently serious breach of a rule of law intended to confer rights on individuals and that a direct causal link exists between the allegedly OLAF’s wrongful act and the harm sustained. To date, compensation has been awarded, for instance, in cases of violation by OLAF of its obligations relating to the processing of personal data, of the principle of the presumption of innocence and of the right to good administration,⁸⁸ for unauthorised leak of confidential information,⁸⁹ as well as for infringement of the right to be heard.⁹⁰ Yet, as rightly noted, even if compensation were granted, such a successful claim would not in itself affects the validity or legality of the act in question.⁹¹

In addition, a person concerned is now entitled under Article 9b to lodge a complaint with the Controller of procedural guarantees (the Controller)

⁸⁵ J. Inghelram, ‘OLAF investigations and fundamental rights: A state of play’, in: M. Luchtman (ed.), *Of Swords and Shields: Due Process and Crime Control in Times of Globalization: Liber amicorum Prof. Dr. J.A.E. Vervaele*, The Hague, The Netherlands, Eleven International Publishing, 2023.

⁸⁶ ECJ, *LG v. Commission*, (no. 64).

⁸⁷ *Ibid.*, § 61.

⁸⁸ ECJ, *OC v. Commission*, 7.03.2024, C-479/22 P.

⁸⁹ ECJ, *Nikolau v. Commission*, 12.09.2007, T-259/03.

⁹⁰ ECJ, *Franchet and Byk v. Commission*, 08.07.2008, T-48/05.

⁹¹ Bovend’Eerdt, (no. 16), p. 183.

regarding OLAF's adherence to procedural safeguards. This includes complaints based on alleged breaches by OLAF of the rules applicable to investigations, notably violations of procedural requirements and fundamental rights.⁹² Importantly, the Controller is an independent body and is appointed by the Commission for a non-renewable term of five years.⁹³ Complaints with the Controller must be filed within one month of the complainant becoming aware of the alleged infringement.⁹⁴ The lodging of a complaint does not have any suspensive effect on the ongoing investigation.⁹⁵ Upon receipt, the Controller reviews OLAF's adherence to procedural guarantees and the rules governing investigations, eventually issuing recommendations on how to resolve the issue.⁹⁶ These recommendations, however, are not legally binding upon OLAF, since the Director-General may decide not to follow them.⁹⁷ The Controller reviews the complaint in an adversarial procedure, ensuring that it does not interfere with the ongoing investigation.⁹⁸

However, it remains uncertain whether a third party, such as an OSP, would have access to this mechanism. If OLAF were to exercise one of the aforementioned powers to request data from OSPs, these would seemingly not be entitled to lodge a complaint with the Controller. Indeed, according to Article 9b of the OLAF Regulation only 'a person concerned', intended as the person suspected and who is therefore under investigation, is entitled to lodge such a complaint.

Finally, data subjects whose rights have allegedly been infringed by unlawful data processing have the right to access to an administrative remedy with the European Data Protection Supervisor under Regulation 2018/1725.⁹⁹ While this right is granted broadly to any data subject who considers that the processing of their personal data infringes the Regulation,¹⁰⁰ this remedy applies exclusively to natural persons. As a result, OSPs are excluded from invoking this remedy.

⁹² Article 9b OLAF Regulation.

⁹³ Article 9a OLAF Regulation.

⁹⁴ Article 9b(2) OLAF Regulation.

⁹⁵ Article 9b(1) OLAF Regulation.

⁹⁶ Article 9b(5) OLAF Regulation.

⁹⁷ Article 9b(7) OLAF Regulation.

⁹⁸ Article 9b(6) OLAF Regulation.

⁹⁹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, pp. 39–98.

¹⁰⁰ Article 63 Regulation 2018/1725.

4. TRANSFER OF DATA BETWEEN PROCEEDINGS

OLAF's responsibility include irregular conduct against the Union's financial interests liable to result in administrative or criminal proceedings.¹⁰¹ It is to attain those objectives that OLAF forwards information to competent authorities in the Member States. Such transmission of information in the context of OLAF's activities may arise in different scenarios. More precisely, such transfer may take place before the initiation of an investigation, during the course of its investigations or after the completion of OLAF's investigative activities. Additionally, in some instances, a transfer from the national competent authorities to OLAF would equally be possible.

4.1. Transfer of information before the opening of an investigation

Firstly, Article 3(12) of the OLAF Regulation provides that OLAF, even before it has decided whether or not to open an external investigation, may liaise with the competent authorities of the Member States concerned to share with them 'information which suggests that there has been a fraud, corruption or any other illegal activity affecting the financial interests of the Union'.¹⁰²

4.2. Transfer of evidence during an investigation

The second case scenario is now covered by Article 12 of the OLAF Regulation. Whenever OLAF, in the course of its investigative activities, considers that punitive action is necessary or appropriate, it has the discretionary power to transmit, in due time, relevant information gathered during the investigation to the competent national authorities. This transfer is intended to enable those authorities to undertake appropriate action in accordance with their respective national legal frameworks.¹⁰³ Upon receipt of such information, national authorities may subsequently initiate their own investigation or integrate the information transmitted by OLAF in an ongoing national investigation. Moreover, OLAF may take part in joint investigation teams established under relevant provisions of Union law, and in that framework, it may share operational information acquired during its investigations.¹⁰⁴

¹⁰¹ Recital 6 OLAF Regulation.

¹⁰² Article 3(12) OLAF Regulation. A similar rule with regard to internal investigations is provided by Article 4(8) of OLAF Regulation. See S. Allegrezza, A. Moraiti, L. Romanò, A. Salemi, 'Information Sharing between the EU Administrative Enforcement Agencies and the Criminal Authorities *Sensu Stricto*', in: Luchtman, Ligeti and Vervaele (eds.), (no.18).

¹⁰³ Article 12(1) OLAF Regulation.

¹⁰⁴ Article 12b, (4), OLAF Regulation.

Conversely, due to limitations of its investigative powers, OLAF may also require the transmission of evidence collected by national authorities in the course of their own investigations.¹⁰⁵ Such transfer of information from the national authorities to OLAF is an EU obligation, except where prohibited by national law.¹⁰⁶ In this cases, the competent authorities of Member States are required, either at OLAF's request or on their own initiative, to transmit without delay any documents or information they hold that pertain to an ongoing OLAF's investigation.¹⁰⁷ This mechanism could thus serve as a means for OLAF to obtain electronic evidence from OSPs indirectly through national authorities, which, in the exercise of their own investigative powers, may have gathered such data.

Another type of transfer of data which may occur in the course of OLAF's investigations involves the European Public Prosecutor's Office (EPPO).¹⁰⁸ In particular, the relationship between the two EU bodies entrusted with the protection of the Union's financial interests shall be based, *inter alia*, on 'information exchange'.¹⁰⁹ Accordingly, OLAF is now required under Article 12c of the OLAF Regulation to report to the EPPO without undue delay, either before or during an investigation, whenever it identifies criminal conduct falling within the EPPO's competence.¹¹⁰ To this end, OLAF must submit to the EPPO a report containing 'as a minimum' certain information exemplified therein.¹¹¹ This provision, therefore, sets out only a non-exhaustive list of information to be transmitted to the EPPO. Notably, it does not preclude OLAF from transferring to the EPPO any electronic evidence it may have gathered in the course of its investigation up to that point. However, the admissibility of such evidence in subsequent criminal proceedings will depend upon compliance with the procedural safeguards provided in Chapter VI of the EPPO Regulation.¹¹²

¹⁰⁵ Bovend'Eerdt, (no. 16), p.144.

¹⁰⁶ Article 8(2), OLAF Regulation.

¹⁰⁷ *Ibid.*

¹⁰⁸ Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017.

¹⁰⁹ Article 1(4a) OLAF Regulation.

¹¹⁰ Article 12c(1) OLAF Regulation. A concrete example is given by the recent investigation into the Member of the European Parliament, Eva Kaili. The OLAF investigation, which was conducted in complementarity with the mandate of the EPPO, was completed on 23 November 2022 and the final report was subsequently sent to the EPPO, online https://anti-fraud.ec.europa.eu/media-corner/news/olaf-statement-recent-media-reports-concerning-european-parliament-2022-12-16_en.

¹¹¹ Notably, a description of the facts, including an assessment of the damage caused or likely to be caused, the possible legal qualification and any available information about potential victims, suspects or other persons involved.

¹¹² See *infra* 4.2.

4.3. Transfer of information upon completion of an investigation

Finally, the transfer of evidence would typically occur upon completion of an investigation through the transmission of the OLAF's final report.¹¹³ This process may occur in various scenarios, both horizontally (between EU institutions, agencies and bodies) and vertically (from OLAF to national competent authorities), and may relate to either an administrative or criminal proceeding.

In particular, since OLAF's tasks are limited to administrative investigations, while subsequent prosecution and sanctioning is in the hands of administrative or judicial authorities, at either the national or EU level, the results of its investigations are naturally meant to flow into a follow-up proceeding. Therefore, equally if not more important to ensure the effective protection of the Union's financial interests is the proper transfer – and subsequent use – of evidence or data collected. Indeed, while OLAF cannot itself establish the liability of the person concerned by its investigations, and lacks any sanctioning powers, it may address recommendations on action to be taken either by EU institutions and bodies or the competent authorities of the Member States.¹¹⁴ Similarly, when information collected by OLAF in an internal investigation reveals the existence of an offence, OLAF's report, together with the recommendations, must be transmitted without delay to prosecutorial authorities of the Member State concerned.¹¹⁵

Additional safeguards regarding the transmission by OLAF of personal data can be found in the OLAF's Guidelines on Data Protection for Investigative Activities.¹¹⁶ In particular, Article 6 outlines the procedures and conditions under which OLAF may share personal data with EU institutions, Member States and third-country authorities, as well as international organisations during the course of its investigations.

Furthermore, the transfer of information may equally involve OLAF as the recipient of data transmitted. This may occur when a judicial authority, in the course of a criminal investigation, realises that a violation does not constitute a criminal offence but rather an administrative irregularity for which an administrative investigation by OLAF may still be appropriate.

This situation is specifically addressed by the EPPO Regulation as regards the transfer of information between the EPPO and OLAF. Recital 105 provides that where the EPPO does not intend to conduct an investigation, it should transmit relevant information to OLAF to enable the latter to take

¹¹³ Article 11 OLAF Regulation.

¹¹⁴ Article 11(1) OLAF Regulation.

¹¹⁵ Article 11(5) OLAF Regulation.

¹¹⁶ OLAF, *Guidelines on Data Protection for Investigative Activities for OLAF Staff*, 25.11.2021,

appropriate action pursuant to its mandate. Specifically, the EPPO may inform OLAF of instances in which there are insufficient grounds to believe that an offence has occurred, yet an administrative investigation by OLAF would still be suitable. Likewise, the EPPO may refer to OLAF cases it has dismissed for administrative follow-up or recovery actions.¹¹⁷ This might involve the transmission of electronic evidence collected by the EPPO from OSPs pursuant to the applicable national criminal procedure, or through European Production Orders, issued in accordance with the provisions of the E-Evidence Regulation, once entered into force. In such cases, it would thus be possible to transfer to OLAF electronic evidence previously collected by the EPPO, thereby enabling OLAF to indirectly obtain data from OSPs.

The issue of the transfer of evidence from criminal to administrative proceedings has already been addressed by the ECJ in *WebMindLicenses*.¹¹⁸ In particular, the question arose as to whether tax authorities could make use in administrative punitive VAT proceedings of records of intercepted communications and emails seized in criminal proceedings. The ECJ ruled that EU law does not preclude administrative proceedings from relying on evidence obtained in the context of a parallel criminal procedure, provided that the rights guaranteed by EU law are observed.¹¹⁹ However, the ECJ highlighted specific duties for the courts in the administrative proceedings.¹²⁰ Notably, national courts reviewing the legality of decisions based on such evidence must first determine whether the investigative measures employed in the criminal investigation were lawful and necessary. Subsequently, they must verify that the use of those evidence by administrative authorities was authorised by law and necessary. Furthermore, courts must ensure the observance of the rights of defence, in particular of the right of access to evidence and of being heard concerning it. However, as previously notes, the legality of OLAF reports and the evidence contained therein may not be subject to direct judicial review before either the EU courts or national courts, thereby questioning whether such a transfer constitutes a legally viable option.

¹¹⁷ Article 39(4) EPPO Regulation.

¹¹⁸ ECJ, *WebMindLicenses kft v. Nemzeti Adó- és Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, 17.12.2015, C-419/14.

¹¹⁹ V. Covolo, 'L'échange d'informations entre autorités administratives et judiciaires. Premiers éclaircissements tirés de l'arrêt *WebMindLicences*, C-419/14', *Eucrim*, no. 3/2016, pp. 146-149.

¹²⁰ Giuffrida, Ligeti, (no. 82).

4.4. Admissibility of data collected from online service providers as evidence

The judicial follow-up of OLAF's investigations has long been the '*Achille's heel*' of the PIF enforcement system.¹²¹ Between 2009 and 2016, fewer than half of OLAF's administrative investigations resulted in prosecution.¹²² The Commission's evaluation identified the primary factor affecting the follow-up of OLAF recommendations as the rules on the admissibility of evidenced by OLAF in national judicial proceedings.¹²³ As a result, the latest amendments to the OLAF Regulation have sought to enhance the judicial follow-up to OLAF's investigations by strengthening the evidentiary value of its final reports.

OLAF's final reports, together with all evidence in support and annexed thereto, now always constitute admissible evidence in all procedures before the ECJ and in administrative proceedings in the EU institutions, bodies, offices and agencies,¹²⁴ as well as in proceedings of a non-criminal nature before national courts and in national administrative proceedings in the Member States.¹²⁵

However, Article 11(2) of the OLAF Regulation maintains the equivalence rule in the context of national criminal proceedings (including punitive administrative proceedings).¹²⁶ This means that OLAF's reports continue to constitute admissible evidence only 'in the same way and under the same conditions as administrative reports drawn up by national administrative inspectors and shall be subject to the same evaluation rules as those applicable to administrative reports drawn up by national administrative inspectors and shall have the same evidentiary value as such reports'.¹²⁷

It follows that reports drawn up by OLAF may be used in national criminal proceedings solely to the extent that they were drawn up in accordance with the rules and procedures laid down by national law.¹²⁸

¹²¹ A. Marletta, 'Interinstitutional Relationship of European Bodies in the Fight against Crimes Affecting the EU's Financial Interests. Past Experience and Future Models', *Eucrim*, no. 3/2016, pp. 141-144.

¹²² Court of Auditors, *Fighting fraud in EU spending: action needed*, Special Report 1/2019, European Union, 2019.

¹²³ European Commission, *Evaluation of the application of Regulation No 883/2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF)*, Final Report, European Union, 2017.

¹²⁴ Article 11(2)(c), OLAF Regulation.

¹²⁵ Article 11(2)(a), OLAF Regulation.

¹²⁶ K. Bovend'Eerd, 'The Commission Proposal Amending the OLAF Regulation', *Eucrim*, no. 1/2018, p. 73.

¹²⁷ Article 11(2)(b), OLAF Regulation.

¹²⁸ J. Vervaele, 'Lawful and Fair Use of Evidence from a European Human Rights Perspective' in F. Giuffrida and K. Ligeti (eds.), (no. 84).

Failure to meet these requirements would render such reports inadmissible in national criminal proceedings. As a result, OLAF-collected evidence is admissible in national criminal proceedings only insofar as they comply with national rules on admissibility of evidence.¹²⁹

The issue has been extensively addressed by Ligeti and Giuffrida.¹³⁰ In general, problems may arise due to differences in procedural safeguards between OLAF's administrative proceedings and national criminal proceedings.¹³¹ Lower safeguards under EU law surrounding the gathering of evidence by OLAF may affect their admissibility in national criminal or punitive administrative proceedings. However, the OLAF Regulation provides now for enhanced protection of fundamental rights and procedural guarantees (see Section 2), thereby making the inadmissibility of OLAF reports and evidence therein less likely.

Finally, the OLAF Regulation now explicitly addresses the admissibility of OLAF's investigative measures, specifically in relation to supporting measures carried out at the request of the EPPO. In this regard, Article 12e(3) of the OLAF Regulation states that when OLAF performs such supporting measures, it must ensure that the applicable procedural safeguards of Chapter VI of the EPPO Regulation are observed. The objective of this provision is clearly to ensure that evidence collected by OLAF can subsequently be used in EPPO criminal proceedings. If so, the same reasoning should apply to any other evidence collected by OLAF and anyhow transferred to the EPPO. By extension, the same reasoning should apply to any other evidence gathered by OLAF and subsequently transmitted to the EPPO. However, no legal provision explicitly addresses the admissibility of evidence unlawfully obtained by OLAF in EPPO proceedings.

5. CONCLUSION

To summarise, OLAF current legal framework appears to offer only limited avenues for OLAF to gather electronic evidence directly from OSPs. In particular, it remains doubtful whether OLAF, *de lege lata*, could directly request data from OSPs in the absence of a clear legal basis. In addition to normative uncertainty, practical challenges persist. Despite the existence of a general duty of cooperation for private entities, OLAF currently lacks the necessary enforcement mechanisms to compel compliance with its requests. This legal gap raises further concerns regarding the practical effectiveness of OLAF's investigatory capacity when dealing with OSPs.

¹²⁹ To this end, Article 11(2) OLAF Regulation clarifies that Member States shall notify OLAF any relevant rules of national law.

¹³⁰ Giuffrida, Ligeti, (no. 82).

¹³¹ *Ibid.*

That is even more true for certain types of data, such as content data and traffic data, whose collection represents a substantial intrusion into fundamental rights. The exercise of such far-reaching powers has the potential to affect the rights of individual concerned, thus requiring strict procedural safeguards. Requests for such data in both punitive administrative and criminal proceedings typically require prior authorisation by a judge or an independent authority. Given these concerns, there is a pressing need for greater legal clarity regarding the possibilities, procedural constraints and specific conditions under which OLAF may request access to such data from OSPs. Any such investigative power must be grounded in a clear and explicit legal basis, ensuring compliance with fundamental rights and procedural safeguards. OLAF's Supervisory Committee itself has already emphasised that if OLAF were to be granted powers similar to those of the European Securities and Markets Authority (ESMA) to request records of telephone and traffic data,¹³² such requests should always be subject to prior judicial approval.¹³³

Over the years, OLAF has undergone continuous evolution, with multiple legislative interventions aimed at adapting its legal framework to emerging challenges. Yet, significant shortcomings remain, most notably, the lack of direct judicial review by EU courts over OLAF's investigative acts. The absence of a mechanism for individuals or entities subject to OLAF's investigatory measures to directly challenge the lawfulness of such acts before EU courts raises concerns about whether such extensive powers could be exercised in the context of OLAF investigations while remaining consistent with the right to effective judicial protection under EU law.

De lege ferenda, it would be advisable to establish a clearer and more explicit legal framework enabling OLAF to request and obtain electronic evidence directly from OSPs. A revised legal basis should clearly delineate the scope, conditions, and procedural safeguards applicable to such requests, ensuring both legal certainty and adequate protection of fundamental rights, particularly with respect to privacy and data protection for the persons concerned, while enhancing the effectiveness of OLAF's investigations.

¹³² M. Siclari, S. Tosza, European Union, in this volume.

¹³³ OLAF Supervisory Committee, Opinion No 2/2017 – Accompanying the Commission Evaluation report on the application of Regulation (EU) of the European Parliament and of the Council No 883/2013 (Article 19), Report, European Union, 2017.

4. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN BELGIUM

V. FRANSSEN and M. VANDORMAEL

1. INTRODUCTION

In recent years, the debate on access to electronic evidence and the role of private actors (such as online service providers (OSPs)) has gained prominence, particularly concerning criminal investigations.¹ Yet, when it comes to punitive administrative (or ‘quasi-criminal’)² investigations, there is much less debate, notwithstanding the fact that access to such evidence can be equally useful and even indispensable to ensure effective investigations. To date, there has been scant research on the legal means to obtain electronic evidence and the cooperation with private actors; moreover there is a lack of understanding of current practices in the field of administrative investigations.

The aim of this chapter is to understand the possibilities for administrative authorities to access electronic evidence from OSPs and other private actors as third parties in the context of punitive administrative proceedings in Belgium. It also seeks to understand to what extent this evidence can be transferred from one administrative proceeding to another, and between administrative and criminal proceedings, both nationally and internationally.

To that end, this chapter focuses on Belgian law and practice in six areas of punitive administrative enforcement (the Analysed Sectors): customs (and

¹ For an overview and comparative analysis of the issues, see V. Franssen, S. Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2025.

² For a more in-depth explanation of ‘quasi-criminal law’, see V. Franssen, C. Harding (eds), *Criminal and Quasi-Criminal Enforcement Mechanisms in Europe: Origins, Concepts, Future*, Hart, 2022.

excise)³ law, VAT law, banking law, financial markets law,⁴ competition law, and data protection law.

This chapter reflects both the legal framework ('law in books') and existing scholarly literature, while also taking into account the practices of the administrative authorities involved in the Analysed Sectors ('law in action'). The analysis of the law in books is based on (traditional) legal desk research (legislation, case law and relevant scholarly literature), while the law in action has been discussed in semi-structured interviews⁵ with representatives from the competent administrative authorities in the Analysed Sectors, private sector stakeholders, and practitioners.⁶ These interviews have proven to be essential for understanding current practices as well as revealing divergent approaches. Indeed, all six sectors represent highly technical fields of law, on which legal scholarship⁷ and (publicly available) case law are rather limited.

Section 2 of this Chapter sets the scene by briefly presenting the competent authorities for each of the Analysed Sectors, their general missions and powers, as well as the nature of their investigations. In the third Section, some general features will be presented. While Belgian law lacks a general framework on (punitive) administrative procedures,⁸ the Analysed Sectors feature a number of common elements. Next, Section 4 will be dedicated to the sectorial framework, analysing the specific powers and rules applicable to the gathering of digital evidence held by private actors, in particular OSPs, to the extent that they exist, and the relevant links with other investigatory

³ In the current legal framework, the enforcement of customs and excise law go hand in hand. For further analysis, see V. Franssen, A. L. Claes, 'Enforcement of Policies against Illicit Trade in Tobacco Products in Belgium', in: S. Tosza, J.A.E. Vervaele (eds), *Combatting Illicit Trade in Tobacco Products*, Springer, 2022, pp. 148 ff.

⁴ We prefer to treat banking law and financial markets law separately as they are governed by different legal frameworks and the enforcement is entrusted with different administrative authorities.

⁵ The interviews were conducted on the basis of a detailed questionnaire which was sent in advance to the interviewees. This questionnaire was common to all sectors, with some minor adjustments for each sector based on preliminary legal desk research, and strongly inspired by the questionnaire prepared by S. Tosza and his team for the country reports. During the interviews, the interviewees could freely add further information. The authors of this chapter both took detailed notes and, where consent was given, the interviews were also recorded for research purposes. The authors are truly grateful to all interviewees for their valuable input. All errors in this chapter are the sole responsibility of the authors.

⁶ For the full list of interviews, see Annex I.

⁷ Scholarly literature on the questions addressed in this chapter is indeed rather limited. Publications usually focus on more general questions.

⁸ M. Pâques, *Droit administratif – Principes généraux*, Larcier, 2024; D. Déom, M-E. Bouchonville, D. Renders, R. Andersen (eds), *Les sanctions administratives*, Bruylant, 2007; J. Put, 'Naar een kaderwet administratieve sancties', *Rechtskundig Weekblad*, 2005, no. 69, pp. 5-7.

powers. Finally, Section 5 will focus on the collaboration of the competent authorities in the Analysed Sectors at the national and international levels with judicial and administrative authorities, and the related question of admissibility of evidence.

2. ADMINISTRATIVE AUTHORITIES IN SELECTED AREAS OF PUNITIVE ENFORCEMENT

To set the scene, this section gives a short overview of these six Analysed Sectors, presenting the competent authorities, their structure, missions and general powers, as well as the nature of the enforcement. The interplay between administrative and criminal enforcement will be discussed further in later parts of this chapter.

Customs law is enforced by the General Administration of Customs and Excise (GACE). The GACE is a very particular kind of administrative authority because it has both administrative and criminal investigatory powers. The applicable legal framework, consisting essentially in the General Act of 18 July 1977 on Customs and Excise,⁹ does not draw a clear-cut distinction between both types of powers. In practice, the administrative powers can be considered limited to first-line inspections.¹⁰ As soon as an actual investigation is needed, the investigation is conducted by the Investigation Unit of the GACE (*Service Enquêtes et Recherches*) and becomes criminal in nature. Unlike other administrative authorities, the GACE has the power to prosecute and to seek criminal sanctions in court, except for imprisonment, which requires the intervention of by the public prosecutor,¹¹ even if the latter was not involved in the investigation. In many criminal proceedings, the GACE and the public prosecutor will thus stand in court shoulder-to-shoulder, even if the latter's role is limited to asking the court to impose a prison sentence.¹² The GACE unit in charge of prosecution is called the *Service Contentieux*. This Prosecution Unit is also in charge of recovering the unpaid customs duties.

The administrative enforcement of VAT law belongs to the competence of the General Tax Administration (GTA) and of its Special Inspection Service (SIS). The division of cases between both entities of the tax administration is not clear-cut; by law, both have the same competences. In practice though, the SIS will essentially investigate (serious) VAT fraud cases, whereas the GTA will investigate any type of case. Depending on the

⁹ General Act of Customs and Excise of 18.07.1977 (General Act of 18.07.1977), *Moniteur belge* (i.e. the Belgian Official Journal) 01.10.1977.

¹⁰ At least, this is how GACE officials themselves define the scope of administrative investigations.

¹¹ Article 281 General Act of 18.07.1977.

¹² For further analysis, see Franssen, Claes (n. 3), p. 182.

importance of the administrative sanctions, enforcement by the tax administration may be punitive in nature. In addition, VAT law can also be enforced through criminal law,¹³ in which case the public prosecutor is in charge of the (rest of the) investigation and the prosecution. In practice, the vast majority of VAT infringements is however dealt with under administrative law.

Competition law is essentially enforced by the Belgian Competition Authority (BCA), through administrative proceedings.¹⁴ The public prosecutor only has limited competence in this area, in particular for bid-rigging.¹⁵ The BCA is an independent administrative authority responsible for enforcing competition policy in Belgium, as stated in the Belgian Code of Economic Law (CEL).¹⁶ The BCA consists of two main bodies or units: the Investigation and Prosecution Unit (*'Auditorat'*)¹⁷ and the Competition College.¹⁸ The Investigation and Prosecution Unit, led by the Competition Auditor General, investigates anticompetitive practices and merger issues. This unit can initiate investigations, respond to complaints, gather evidence, propose settlements, or refer cases to the Competition College.¹⁹ The latter has the authority to impose sanctions.²⁰ Decisions by the Competition College can be appealed to the Market Court.²¹ While the procedure is administrative under domestic law, the BCA fully acknowledges the punitive and thus criminal nature of its fines and ensures the respect of procedural rights applicable in criminal matters, in line with the case law of the Court of Justice of the EU (CJEU).²² The criminal nature of competition law proceedings has also been acknowledged by Belgian courts, leading to certain changes in the proceedings (e.g. need for *ex ante* judicial authorisation for dawn raids, see 4.2.5.).

The enforcement of financial markets law has essentially been entrusted to the Financial Services and Markets Authority (FSMA), an autonomous public body,²³ even if certain infringements are also criminal offences (e.g.

¹³ Article 73-74ter VAT Code of 03.07.1969 (VAT Code), Moniteur belge 17.07.1969.

¹⁴ Article IV.28 CEL.

¹⁵ Article 314 Criminal Code of 08.06.1867 (Criminal Code), Moniteur belge 09.06.1867.

¹⁶ Article IV.16, § 1 CEL.

¹⁷ Article IV.26 CEL.

¹⁸ Article IV.21 CEL.

¹⁹ Article IV.28 CEL.

²⁰ Article IV.52 CEL.

²¹ Article IV.90 CEL.

²² For further analysis from a European perspective, see V. Franssen, S. Vandeweerd, 'Supranational Administrative Criminal Law', *Revue internationale de droit pénal*, 2019, no. 90, pp. 18-28 and 58-66.

²³ Article 44 Act of 02.08.2002 on the supervision of the financial sector and on financial services (Act of 02.08.2002), Moniteur belge 04.09.2002.

insider dealing), in conformity with the Market Abuse Directive of 2014.²⁴ The FSMA is responsible, amongst others, for the regulation of financial products, for market supervision and supervision of service providers, and for the enforcement of conduct rules.²⁵ Its operations are carried out through the Management Committee,²⁶ the Investigation and Prosecution Unit (*Auditorat*)²⁷ and the Sanctions Committee.²⁸ The FSMA possesses significant administrative powers to investigate and sanction non-compliance within the financial markets, as regulated under the Act of 2 August 2002 and the Market Abuse Regulation²⁹ (MAR). The FSMA's enforcement actions focus primarily on the imposition of fines and other penalties to uphold market integrity. Decisions of the Sanctions Committee can be appealed to the Market Court.³⁰ The FSMA recognizes the punitive (hence criminal) nature of its fines and adheres to the procedural rights laid down in the European Convention on Human Rights (ECHR).³¹

The enforcement of banking law is within the purview of the National Bank of Belgium (NBB).³² The NBB's primary function is to ensure the prudential supervision of credit institutions, safeguarding their stability and regulatory compliance.³³ As an autonomous public institution, the NBB comprises several units, including the Management Committee,³⁴ the Investigation and Prosecution Unit,³⁵ and the Sanctions Committee.³⁶ The Investigation and Prosecution Unit is tasked with investigating administrative offences,³⁷ while the Sanctions Committee is responsible for imposing corrective measures and sanctions on financial institutions.³⁸ These sanctions are considered criminal in nature in the meaning of Article 6 of the ECHR

²⁴ Directive 2014/57/EU of the European Parliament and of the Council of 16.04.2014 on criminal sanctions for market abuse (Market Abuse Directive), OJ L173/179, 16.04.2014.

²⁵ Article 45 Act of 02.08.2002.

²⁶ Article 71 Act of 02.08.2002.

²⁷ Article 70 Act of 02.08.2002.

²⁸ Article 72, § 3 Act of 02.08.2002.

²⁹ Regulation (EU) 596/2014 of the European Parliament and of the Council of 16.04.2014 on market abuse (Market Abuse Regulation), OJ L173/1, 16.04.2014.

³⁰ Article 120 Act of 02.08.2002.

³¹ Cass. (i.e. Belgian Supreme Court), 10.02.2023, no. C.22.0184.N.; Article 70 § 1bis, 2° Act of 02.08.2002.

³² Unlike the project questionnaire, this chapter prefers to split banking law and financial markets law as the legal framework, competent authorities, powers, and sanctions differ.

³³ Articles 8 and 12 Act of 22.02.1998 establishing the organic statute of the National Bank of Belgium (Act of 22.02.1998), *Moniteur belge* 28.03.1998.

³⁴ Articles 19 and 12 Act of 22.02.1998.

³⁵ Article 21 §1 Act of 22.02.1998.

³⁶ Article 21 ter Act of 22.02.1998.

³⁷ Articles 21bis and 36/19 Act of 22.02.1998.

³⁸ Article 12ter Act of 22.02.1998.

and in line with EU law.³⁹ This has also been confirmed by the Sanctions Committee (e.g. with respect to the application of the *nemo tenetur* principle).⁴⁰ The decisions taken by the Sanctions Committee may be appealed to the Market Court.⁴¹

Data protection law is enforced by the Belgian Data Protection Authority (DPA). The DPA succeeded the Belgian Privacy Commission, which was an advisory authority without enforcement powers.⁴² As an independent administrative authority, the DPA is tasked with ensuring compliance with data protection legislation.⁴³ It is composed of various bodies, including the General Secretariat,⁴⁴ a Knowledge Centre,⁴⁵ the First-Line Service,⁴⁶ the Inspection Service,⁴⁷ the Litigation Chamber,⁴⁸ and the Management Committee.⁴⁹ The Inspection Service, led by the Inspector General, investigates complaints and potential data protection violations.⁵⁰ The Litigation Chamber resolves disputes and can impose corrective measures and fines.⁵¹ These sanctions are considered criminal in nature under Article 6 of the ECHR. The decisions by the Litigation Chamber may also be appealed to the Market Court.⁵²

In conclusion, the foregoing introductory presentation suggests both diversity and convergence among the Analysed Sectors, the latter at least for the last four which are all heavily influenced by EU law. Some of those common features will be further discussed in Section 3.

3. PUNITIVE ADMINISTRATIVE PROCEEDINGS: LACK OF GENERAL FRAMEWORK, TENTATIVE CATEGORISATION

Before discussing the specific powers and measures regarding digital evidence gathering, it is important to point out that there is no overarching legal framework in Belgium governing all administrative regimes with

³⁹ For further analysis from a European perspective, see Franssen, Vandeweerd, (n. 22), pp. 28-44 and 66-71.

⁴⁰ Decision of the NBB Sanctions Committee, 02.06.2023, § 14 ff. (in particular § 18).

⁴¹ Article 36/21 Act of 22.02.1998.

⁴² Article 3 Act of 03.12.2017 establishing the Data Protection Authority (Act of 03.12.2017), Moniteur belge 10.01.2018.

⁴³ Article 4 Act of 03.12.2017.

⁴⁴ Article 7, 2° Act of 03.12.2017.

⁴⁵ Article 7, 4° Act of 03.12.2017.

⁴⁶ Article 7, 3° Act of 03.12.2017.

⁴⁷ Article 7, 5° Act of 03.12.2017.

⁴⁸ Article 7, 6° Act of 03.12.2017.

⁴⁹ Article 7, 1° Act of 03.12.2017.

⁵⁰ Articles 28-31 Act of 03.12.2017.

⁵¹ Articles 32-34 Act of 03.12.2017.

⁵² Article 108 Act of 03.12.2017.

punitive aspects. While Belgian administrative law and general principles are well established, they do not specifically address issues related to punitive administrative investigations, powers, and sanctions.⁵³ Instead, these rules are typically defined on a sector-by-sector basis.

This sector-specific approach results in a lack of uniformity regarding critical aspects such as the powers of competent authorities and the exchange of information between authorities. Each sector operates under its own rules and practices, leading to inconsistencies and a fragmented legal landscape and divergent practices. In certain respects, the sectorial legal framework remains silent (e.g. the admissibility of evidence), forcing authorities and courts to reason by analogy, drawing inspiration from criminal procedure (see 4.3.). Moreover, Belgian law does not provide a general framework for the interaction between administrative and criminal enforcement, which is dictated by sector-specific legislation and practices that vary significantly (see 4.2.).

As a result, the landscape of punitive administrative law in Belgium is marked by a lack of cohesion and standardized procedures, reflecting a complex and inconsistent regulatory environment. A sector-specific analysis is, therefore, the most relevant approach to understanding the mechanisms for collecting digital evidence from third parties, including OSPs.

That said, even if there is no general framework on punitive administrative enforcement under Belgian law, it is possible to identify a number of common features across the Analysed Sectors, at least those that have been created over the last decennia under the influence of EU legislation, in particular: competition law, financial markets law, banking law, and data protection law. Those sectors are profoundly marked by EU law and structured in a comparable way. They exhibit similar organisational and procedural frameworks, providing for largely comparable investigatory powers and punitive measures. EU law thus fosters a semblance of standardisation concerning punitive administrative procedures in those sectors. That said, despite a few common traits, the sectorial analysis (see 4.) will also reveal some important differences, notably with respect to certain powers regarding OSPs. In addition to that, the reality on the ground remains one of vast disparities among the different administrative authorities, even in the presence of similar legislations, be it in terms of resources, actual use of powers, and/or practices.

In contrast, VAT law is primarily shaped by national legal paradigms, even if it increasingly undergoes EU law influence. Indeed, punitive

⁵³ Telling in this respect is that one of the main handbooks on Belgian administrative law dedicates only 25 pages to the subject matter of punitive administrative law (on a total of 1316 pages): Pâques, (n. 8), pp. 683-708.

administrative enforcement of VAT law strongly resembles other subsectors of tax law, such as income tax.

Finally, the hybrid enforcement of customs law is highly a derogatory and self-standing regime, despite the existence of the Union Customs Code.⁵⁴ This sector operates in relative isolation, devoid of influence or resemblance to other punitive administrative legal regimes, be it at the national or at the EU level.

Therefore, the enforcement approach in the last two fields diverges considerably from the one adopted in the other four Analysed Sectors, as the following sections of this chapter will show.

4. PUNITIVE ADMINISTRATIVE PROCEEDINGS: SECTORIAL FRAMEWORK

4.1. Introduction

In the absence of a uniform legislative framework, a sector-specific analysis of the law and practices of each administrative authority is crucial to understand how the competent authorities eventually request evidence from OSPs and other private actors as third parties. The following subsections will provide an analysis of each sector's specific investigatory powers, the types of data and/or information the competent authorities can request, and their enforcement practices. Before kicking off the analysis, it is useful to make a few general preliminary observations.

First of all, it should be noted that the term 'online service providers' is not used by Belgian law in any of the Analysed Sectors. Instead, the law often refers to 'any person' without specifying. While this leaves quite some flexibility as to the personal scope of application of the investigation measures, in practice the measures are usually only applied toward suspects, not third parties. In a few instances, the law provides for specific powers concerning the production of data held by operators and providers of electronic communications services. Interestingly, these provisions use the same terminology as the Code of Criminal Procedure⁵⁵ (CCP). This does however not necessarily mean that their scope is also identical in practice.

To the extent that a punitive administrative investigation can turn into a criminal investigation (see 5.1.2.), it is worth noting that the CCP also refers to 'any person' with respect to certain cooperation duties (such as the obligation to provide access information or more active technical assistance to a judicial authority conducting a search in an information system).⁵⁶ With

⁵⁴ Regulation (EU) 952/2013 of the European Parliament and of the Council of 09.10.2013 laying down the Union Customs Code, OJ L269/1, 09.10.2013.

⁵⁵ Code of Criminal Procedure of 17 November 1808, Moniteur belge 27.11.1808.

⁵⁶ Article 88quater, §§ 1-2 CCP.

respect to (data) production orders, the CCP uses the term ‘operator of a network of electronic communications’ and refers in addition to ‘any person who provides, in the Belgian territory, in whatever way, a service consisting in transmitting signals via a network of electronic communications (...)’, including the ‘provider of an electronic communications service’.⁵⁷ The latter terms are however not defined by the CPP and their meaning may differ from the one used in other branches of the law, due to the principle of (conceptual) autonomy of the criminal law.

Second, as regards the territoriality of the investigation measures and cooperation duties, the law is usually not very explicit. In principle, the powers of Belgian authorities are limited to the Belgian territory, by virtue of the principle of territoriality and national sovereignty. While the rules in the CCP are sometimes more far-reaching and produce extraterritorial effects, in particular with regard to investigation measures concerning information systems (e.g. the search of an information system)⁵⁸ and the cooperation of service providers (i.e. by applying the criterion of the territory in which the service is provided, regardless of the establishment of the service provider),⁵⁹ the powers of the administrative authorities are effectively limited to the Belgian territory – except for some nuances explained below (see e.g. VAT law). When seeking information or data held by a person who is not (physically) present in Belgium, the authorities will thus in principle address their foreign counterparts, following the rules on mutual administrative assistance, to obtain the information or data (see also 5.2.).

Third, another common feature of the six Analysed Sectors is that there are no specific rules on ‘transfer of data’. If an administrative authority has the power to seize or to order the production of data, the law will of course determine the conditions for doing so. But these rules are not conceived a ‘data transfer’ rules.

⁵⁷ Article 46bis, § 1, para. 1, Article 88bis, § 1, para. 1 and Article 90quater, § 2 CCP. For further analysis, see S. Careel, F. Verbruggen, ‘Digital Evidence in Criminal Matters: Belgian Pride and Prejudice’ in: V. Franssen, S. Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2025, pp. 237-246.

⁵⁸ M. Corhay, ‘L’extension de la recherche dans un système informatique : du droit belge à la Convention de Budapest sur la cybercriminalité’, *Journal des Tribunaux*, 2020, pp. 133-141.

⁵⁹ For an analysis of those rules, see e.g. V. Franssen, ‘The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?’, *European Data Protection Law Review*, 2017, pp. 534-542; Careel, Verbruggen, (n. 57), pp. 229-236.

4.2. Requests for evidence to online service providers (and other private actors as third parties)

4.2.1. Customs enforcement

As explained, the GACE is in charge of the investigation in customs law cases. The General Act of 18 July 1977, which defines the main powers and sanctions applicable to customs infringements, is a complicated and rather old piece of legislation, which is essentially based on an even older Act of 26 August 1822.⁶⁰ This legal framework clearly predates the digital revolution, even if some punctual amendments have been made in recent years. Under this law, the powers of the GACE are broad and derogate substantially from the ones laid down in the CCP, meaning they provide for less procedural safeguards. For example, within a specific customs zone called '*le rayon des douanes*',⁶¹ the powers of the customs administration are broader and do not require *ex ante* judicial authorisation, not even for the search of private premises.⁶² The powers of the GACE are, of course, limited to the Belgian territory. The administrative or criminal nature of these powers, which are presented in a scattered way in the General Act of 18 July 1977, is however not clearly expressed in the law.

In addition to that specific legal framework, certain officials of the GACE can be vested with the powers of 'officer of judicial police' ('*officier de police judiciaire*').⁶³ This holds true for (criminal) offences affecting the financial interests of the EU as well as any offence relating to the import, export or transit of goods. With the title of officer of judicial police comes a whole range of investigative powers that are laid down in the CCP, including certain special investigative techniques (i.e. undercover operations). These powers are, however, exercised under the authority of the public prosecutor

⁶⁰ Act of 26.08.1822 on Customs and Excise Offences, Staatsblad (i.e. the Dutch Official Journal) no. 38. This Act was adopted when Belgium was still a part of the Netherlands.

⁶¹ The customs zone is an area 'along the maritime coast that extends inland for five kilometres from the low tide line' and that comprises also 'the territory of customs seaports and customs airfields as well as an area outside this territory with a width of 250 m from the limits of this territory' (Article 167 Act of 22.04.1999 concerning the Exclusive Economic Zone of Belgium in the North Sea, Moniteur belge 10.07.1999).

⁶² Articles 173 and 174 General Act of 18.07.1977. In case of '*flagrant délit*' (i.e. the author is caught red-handed, while committing the offence), Article 175 also allows for the search of the private premises where the goods have been entered, even if these premises are located elsewhere in the territory, beyond the indicated customs zone. Once more, there is no need for judicial authorisation. In other situations, a search of private premises requires a judicial authorisation of the Traffic Court (Article 197 General Act of 18.07.1977), yet without requiring the opening of a judicial inquiry, whereas this is the rule in criminal proceedings (Article 28septies CCP).

⁶³ Article 3 Act of 22.04.2003 granting certain officers of the Customs and Excise Administration the status of judicial police officer, Moniteur belge 08.05.2003.

(potentially the European Public Prosecutor's Office (EPPO)) in the context of a preliminary inquiry, or in case of a judicial inquiry, under the authority of an investigating judge. In other words, in such case, the investigation is governed by the rules on criminal procedure.

Specifically, with regard to electronic evidence and the cooperation with private actors as third parties, the legal framework applicable to the GACE provides very little information. For instance, Article 203, § 1 of the General Act of 18 July 1977 states that importers, exporters and 'any person who is directly or indirectly interested by the import, export or transit of goods' are required to communicate 'any invoice, letter, accountancy document, inventory, register, document or correspondence related to their professional activity and whose production is considered necessary' to the GACE. In practice, it appears this legal basis is also used to require data from operators of electronic communications services, even if this is not at all obvious from the wording of the legal text. No (*ex ante*) judicial authorisation or (*ex post*) judicial control is required nor provided; Article 203, § 1 only states that the GACE official must have at least the rank of financial expert.

Article 203, § 2 of the General Act of 18 July 1977 continues by stating that GACE officials have the right to make a copy or to retain documents and correspondence that (may) prove the existence of the customs offence. If the documents are kept in a digital manner, GACE officials have the right to determine the form in which they want to receive the documents.

Non-cooperation of third parties with such orders does not seem to be sanctioned explicitly, unless the residual 'catch-all' Article 261 of the General Act of 18 July 1977 would be applied,⁶⁴ as opposed to the harsh legal regime that applies to economic operators, customs representatives and declarants who all risk to be subject to far-reaching measures (e.g. seizure of goods, boats or other means of transportation)⁶⁵ and severe sanctions (e.g. fines amounting to five to ten times the evaded customs duties)⁶⁶ if they can be linked to the customs offence. This risk is compelling enough to ensure cooperation throughout the investigation.

By 'joggling' the powers laid down in the General Act of 18 July 1977 and those attributed to officers of judicial police, customs officials can conduct a wider variety of investigation measures. For instance, under Article 39ter of the CCP, they could order the preservation (or 'quick freeze') of data stored, processed or transmitted by means of an information system that are particularly vulnerable to loss or modification to any natural or legal person

⁶⁴ According to this legal provision, any violation of the customs legislation is punished with a fine of 125 up to 1.250 euros, if the behaviour is not incriminated by another legal provision. See also Franssen, Claes, (n. 3), p. 147.

⁶⁵ Articles 221-222 General Act of 18.07.1977.

⁶⁶ See e.g. Article 221, § 1 General Act of 18.07.1977.

who possesses or controls the data. It suffices that this person has a virtual presence on Belgian territory.⁶⁷ They may also search and seize data that is stored on a device (e.g. a cellphone or computer), provided that the investigation would be led by a judicial authority (public prosecutor or investigating judge).⁶⁸ According to discussions with customs officials, the production of identification⁶⁹ and metadata⁷⁰ (i.e. traffic and location data) by providers of electronic communications services would also be possible, though once again only if the investigation is conducted under the authority of a judicial authority.⁷¹ In such case, the investigation is of course clearly criminal in nature, both in the meaning of Article 6 of the ECHR and under domestic law. Put differently, such powers exceed the realm of ‘punitive administrative’ enforcement.

Legal remedies under the General Act of 18 July 1977 are quite limited. For instance, there is no right to access to the case file,⁷² and the right to ask for the restitution of seized goods is limited to goods (*‘marchandise’*);⁷³ nothing is provided for documents (or data) that have been seized by or produced to the GACE. In contrast, if a GACE official vested with the powers of ‘officer of judicial police’ acts under the authority of a judicial authority, the legal remedies of the CCP are logically applicable.⁷⁴

In sum, the possibilities for the GACE to gather electronic evidence from private parties such as OSPs are quite limited under the General Act of 18 July 1977, notwithstanding the Act provides for far-reaching investigation powers. The traditional focus on ‘goods’ entering the territory is still predominant in this legislation. The only relevant power seems to be the one laid down in Article 203 of the General Act of 18 July 1977, whose wording is not very explicit when it comes to third parties.

4.2.2. Tax enforcement as regards VAT

The powers of the tax administration are laid down in the VAT Code. These powers essentially concern taxpayers, i.e. the persons who are subject

⁶⁷ V. Franssen, O. Leroux, ‘Recherche policière et judiciaire sur internet: analyse critique du nouveau cadre législatif belge’, in: V. Franssen, D. Flore (eds), *Société numérique et droit pénal. Belgique, France, Europe*, Larcier/Bruylant, 2019, pp. 165-173.

⁶⁸ Article 39ter, § 2 CCP.

⁶⁹ Article 46bis CCP.

⁷⁰ Article 88bis CCP.

⁷¹ Explanatory Memorandum to the Act of 22.04.2003, Doc. Parl., Ch. Repr., sess. ord. 2020-2021, no. 50-2249/001, p. 9.

⁷² Even if interested persons can of course ask for such access, their request is systematically refused and there is no appeal against the GACE’s decision.

⁷³ Article 275 General Act of 18.07.1977.

⁷⁴ For an analysis of legal remedies with regard to electronic evidence gathering in criminal investigations, see Careel, Verbruggen, (n. 57), pp. 246-251.

to VAT obligations (and thus, in principle, the persons under investigation), not private actors as third persons.

One of those obligations is the duty to keep a copy of all invoices, whether emitted or received, for a period of ten years.⁷⁵ Invoices may be kept electronically or on paper, as long as the authenticity can be guaranteed.⁷⁶ Logically, the tax administration may then ask the production of those invoices, as well as any other document that must be legally retained.⁷⁷ In case the documents are stored electronically, it is irrelevant whether the ‘data’⁷⁸ is stored in Belgium or abroad (e.g. using a cloud computing service).⁷⁹ But the person in point must be either established in Belgium or subject to VAT in Belgium.⁸⁰ In case of a foreign person without an establishment or a legal representative in Belgium, the tax administration must be informed of the address in Belgium where the invoices and other relevant documents can be consulted and handed over if the administration requests so.⁸¹

Next, ‘any person’ can be ordered to provide information (*‘renseignements’*) to the VAT administration.⁸² In practice, this power is used with respect to taxpayers and any person involved in the chain of goods or services subject to VAT. Hence, it may concern certain service providers or online platforms (e.g. in the e-commerce sector). In theory, this power could also be used to obtain electronic communications data or other data from OSPs and other private actors as third parties, but in practice that does not seem to be the case. Should the need for such data however arise in the future, this legal basis could be used for that purpose, without requiring any amendment.⁸³

While the VAT Code does not provide for sanctions in case of refusal to provide the requested documents or information, the VAT administration can of course decide to use more coercive powers and conduct a search of premises to search for and seize the requested documents or information.⁸⁴ Such search does not require an *ex ante* judicial authorisation, unless if the search (also) concerns inhabited premises. In the latter case, the search is only

⁷⁵ Article 60, § 1 and § 3 VAT Code.

⁷⁶ Article 60, § 6.

⁷⁷ Article 61, § 1 VAT Code.

⁷⁸ Interestingly, the law uses the term *‘données’* here, whereas the rest of the legal provision refers to ‘invoices’, ‘accounting books’ or other ‘documents’. But it is clear that reference is made to the ‘data’ concerning those documents.

⁷⁹ Article 61, § 3 VAT Code.

⁸⁰ Article 61, § 1, para. 3 VAT Code.

⁸¹ Article 61, § 1, para. 7 VAT Code.

⁸² Article 62, para. 1 VAT Code.

⁸³ The officials of VAT administration we interviewed were quite affirmative on this point.

⁸⁴ Article 63, para. 1 VAT Code.

possible between 5 am and 9 pm, and upon a warrant issued by the traffic court (*'tribunal de police'*).⁸⁵

Finally, like customs officials (see 4.2.1.), officials of the VAT administration can be vested with the powers of 'officer of judicial police'.⁸⁶ In that capacity, they can participate in a criminal investigation conducted under the authority of a judicial authority (in VAT cases, this usually is the public prosecutor), provided that the investigation concerns a VAT offence or money laundering, especially when committed in the context of a criminal organisation.⁸⁷

4.2.3. Punitive enforcement in the area of financial markets law

As explained in Section 2, the FSMA is vested with comprehensive investigative powers designed to uphold the integrity of financial markets in Belgium.⁸⁸ The Auditor and Deputy Auditor of the FSMA can exercise all investigative powers granted by relevant laws and regulations.⁸⁹ These powers are essential for fulfilling the FSMA's regulatory responsibilities. The list of investigatory powers includes various general powers, such as the possibility to request any information and documents from any natural or legal person⁹⁰ and to verify the accuracy of information provided,⁹¹ the power to summon and question any person,⁹² and the power to order, with the prior consent of an investigating judge, (i) a provisional seizure of goods (including electronic devices), assets, funds, securities, titles or rights belonging to the person who is the subject of an investigation by the FSMA and (ii) a temporary ban on exercising professional activities.⁹³ Some of those general powers can also be useful to obtain information or data stored by OSPs.

More interesting are the powers:

- to ask the operator or provider of an electronic communications network or service to (i) identify the subscriber or the habitual user of an electronic communications service; or (ii) pass on identification data relating to the electronic communications services to which a given person subscribes, or which are habitually used by a given person (i.e. the production of identification data),⁹⁴ and

⁸⁵ Article 63, para. 3 VAT Code.

⁸⁶ Article 63ter, § 1 VAT Code.

⁸⁷ Article 63ter, § 2 VAT Code.

⁸⁸ Article 45 Act of 02.08.2002.

⁸⁹ Article 70, § 1 Act of 02.08.2002.

⁹⁰ Article 78 Act of 02.08.2002.

⁹¹ Article 78 Act of 02.08.2002.

⁹² Article 79 Act of 02.08.2002.

⁹³ Article 82 Act of 02.08.2002.

⁹⁴ Article 81 Act of 02.08.2002.

- to request, with the prior consent of an investigating judge, the collaboration of the same persons to (i) have the call data traced on electronic communications devices from which, or to which, calls have been made; (ii) have the origin or destination of electronic communications identified (i.e. the production of metadata).⁹⁵

The latter two powers are particularly relevant when seeking to understand how the FSMA gathers electronic evidence from private actors such as OSPs. Since 2017, the Act of 2 August 2002 uses the same terminology as the CCP,⁹⁶ that is operators of electronic communications networks and any other person who provides an electronic communications service on Belgian territory, even if this provider has not infrastructure or establishment in Belgium. Mere virtual presence in Belgium is, in principle, enough. As discussed elsewhere, the production orders of the CCP have extraterritorial reach and are frequently applied by Belgian judicial authorities in criminal investigations.⁹⁷ Moreover, this approach has inspired the EU legislator when adopting the e-Evidence Regulation.⁹⁸ Interestingly though, contrary to the judicial authorities, the FSMA does not use these powers toward foreign service providers, notwithstanding the wording of Articles 81 and 84 of the Act of 2 August 2002. The FSMA does not seem to be fully aware of the existing case law and practice relating to these orders in criminal procedure. In practice, the FSMA's jurisdiction is thus (more strictly) limited to the Belgian territory. Instead, when dealing with foreign providers or data located outside Belgium, the FSMA often resorts to seizing electronic devices (located in Belgium) on which the data is stored to access the required information (see above). This approach underscores the challenges posed by cross-border investigations, particularly with services like Gmail or WhatsApp, which are widely used, also for professional use. Notwithstanding those challenges, the Auditor considers the investigatory powers provided by law adequate, enabling the FSMA to obtain the necessary information in most investigations.

The FSMA's broad powers obviously come with a number of procedural safeguards, such as the requirement of an *ex ante* authorisation of an investigating judge in some instances. Moreover, its investigatory measures must: (i) respect the guarantees provided for by Article 6 of the

⁹⁵ Article 84 Act of 02.08.2002.

⁹⁶ Articles 46bis, § 1, para. 2 and 88bis, § 1, para. 2 CCP.

⁹⁷ Franssen, (n. 59), 2017, pp. 534-542; Careel, Verbruggen, (n. 57), pp. 229 ff.

⁹⁸ Regulation (EU) 2023/154 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L191/118, 12.07.2023.

ECHR;⁹⁹ (ii) fall within the scope of the Auditor's investigation mandate;¹⁰⁰ (iii) respect the principles of proportionality and necessity;¹⁰¹ and (iv) comply with the general principles of administrative law.

Although the FSMA has broad investigatory powers, it lacks cannot exercise coercion on suspects, who have the right to remain silent or refuse to provide information.¹⁰² Others may face fines and penalties for non-collaboration.¹⁰³

Individuals subject to FSMA investigations can challenge investigative actions before the Market Court,¹⁰⁴ particularly concerning the admissibility or scope of evidence. However, as will be explained below (see 5.3.), disputes over evidence admissibility are rare, largely due to the FSMA's well-established regulatory framework and authority in an area where one's professional reputation plays an important role. That often discourages undertaking legal challenges.

4.2.4. Punitive enforcement in the area of banking law

The NBB is endowed with comprehensive investigative powers, which are essential for its role in ensuring the prudential supervision of credit institutions. These powers are defined and circumscribed by the legislative framework that governs the NBB's operations, particularly in the Act of 18 September 2017¹⁰⁵ and the Act of 22 February 1998. The Auditor of the NBB possesses the authority to summon and interview individuals, as well as to request necessary information from entities and third parties involved in specific operations or activities.¹⁰⁶ This power is crucial for verifying compliance with relevant laws and regulations, including those under international cooperation agreements. However, it is important to note that these powers are inherently tied to the NBB's overarching mandate to ensure the sound functioning of credit institutions.

The investigative approach of the NBB is primarily designed to guarantee the proper organisation and functioning of the institutions under its supervision. Unlike the FSMA, which may engage in the detection of

⁹⁹ Cass., 10.02.2023, No C.22.0184.N.; Article 70, § 1bis, 2° Act of 02.08.2002.

¹⁰⁰ Article 70 Act of 02.08.2002.

¹⁰¹ Article 81 Act of 02.08.2002.

¹⁰² S. Benzidi, F. Lefèvre, *Gros plan sur la FSMA: Chronique de jurisprudence depuis la création de la Commission des sanctions à nos jours*, Larcier, 2021, pp. 218-223; Decision of the FSMA Sanctions Committee, 28.04.2010.

¹⁰³ Article 86 Act of 02.08.2002.

¹⁰⁴ Article 120 Act of 02.08.2002.

¹⁰⁵ Act of 18.09.2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash, Moniteur belge 06.10.2017.

¹⁰⁶ Article 91 Act of 18.09.2017.

individual misconduct such as insider trading, the NBB's focus remains on ensuring that the institutions adhere to legal and regulatory standards. The NBB's investigations are therefore more concerned with assessing and rectifying organisational deficiencies, internal procedures, and governance issues within these entities. As a result, the nature of its investigations is less about the detection of violations and more about ensuring compliance with the regulatory framework.

Under its current legislative mandate, the NBB does not possess the legal authority to directly access data from OSPs. However, it does have the authority to 'hear any person',¹⁰⁷ which can be interpreted to extend to third parties, potentially including OSPs. Despite this, the NBB has not exercised this prerogative to obtain data from OSPs.

In fact, the NBB considers the authority to access electronic evidence from OSPs largely unnecessary for its purposes. This is primarily due to the nature of its supervisory mission, which typically involves direct engagement with the supervised entities. As indicated, NBB investigations focus on the operational aspects of those entities (organisational structure, internal procedures, governance), which generally demonstrate a willingness to cooperate. That further reduces the need for the NBB to seek evidence from external parties like OSPs.

The distinct focus of the NBB's investigations, centered on institutional compliance rather than individual misconduct, also differentiates its methods, results, and potential sanctions from those of the FSMA. While procedural similarities exist between the two bodies, the NBB's unique competence to ensure the soundness of credit institutions shapes its investigatory approach and the extent to which it utilises its powers.

4.2.5. Competition law enforcement

The BCA is equipped with extensive investigative powers, primarily exercised by its Investigation and Prosecution Unit.¹⁰⁸ These powers include the ability to gather evidence through dawn raids¹⁰⁹ and requests for information,¹¹⁰ as outlined in the CEL. Additionally, the Investigation and Prosecution Unit can conduct interviews with individuals as part of its inquiries.¹¹¹ Dawn raids, which involve the search of premises, are the preferred method due to the control they provide over the data collection process. Considering the intrusive nature of dawn raids, they require respect

¹⁰⁷ Article 36/9, § 1 Act of 22.02.1998.

¹⁰⁸ Article IV.28 CEL.

¹⁰⁹ Article IV.41, § 3 CEL.

¹¹⁰ Article IV.41, §§ 2-3 CEL.

¹¹¹ Article 40/1 CEL.

for additional procedural safeguards, such as the prior authorisation of an investigating judge and adherence to the principle of proportionality.¹¹² The legality and scope of dawn raids can be contested before the Market Court.¹¹³

The BCA places significant emphasis on the collection and processing of electronic evidence, which has become central to modern antitrust investigations. During dawn raids, the BCA is authorised to seize any electronic data accessible to the entity under investigation, regardless of its storage location. As remote working and cloud services have become increasingly common, the BCA deploys larger, more specialised teams during these raids. To ensure targeted searches, the BCA employs a predefined list of keywords, ensuring that only relevant data is seized.

Since January 2023,¹¹⁴ the BCA has also been granted the authority to request traffic data, location data, and other electronic records from communications operators,¹¹⁵ similar to the powers of the FSMA (see 4.2.3.). Nevertheless, this power has not yet been used widely. More generally speaking, cooperation with private actors in obtaining electronic evidence has thus far been limited to the entities which are directly under investigation.

4.2.6. Data protection law enforcement

The DPA too is vested with broad investigative powers to ensure compliance with data protection laws, particularly the General Data Protection Regulation¹¹⁶ (GDPR) and related national law. The DPA's Inspection Service, a key division, is responsible for conducting those investigations. The Inspector General and his team of inspectors have a wide range of investigative tools, crucial for enforcing data protection regulations effectively. These powers, laid down in the Law of 3 December 2017,¹¹⁷ include the identification of individuals,¹¹⁸ conducting interviews,¹¹⁹

¹¹² Article IV.40, § 1 and Article IV.40, § 1/1.

¹¹³ Article IV.90 CEL.

¹¹⁴ Act of 25.09.2022 containing various provisions on economic matters, *Moniteur belge* 16.01.2023.

¹¹⁵ The Act of 25.09.2022 grants the auditor the authority to request telecommunications operators to provide data related to traffic, location, identification, and the IP addresses of their clients; Article IV.40, § 1/1 CEL. See also Belgian Competition Authority, *Annual Report 2023, 2024*, p. 31.

¹¹⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L119/1, 27.04.2016.

¹¹⁷ Act of 03.12.2017 establishing the Data Protection Authority (Act of 03.12.2017), *Moniteur belge* 10.01.2018.

¹¹⁸ Article 66, § 1, 1° Act of 03.12.2017.

¹¹⁹ Article 66, § 1, 2° Act of 03.12.2017.

initiating written inquiries,¹²⁰ performing on-site inspections,¹²¹ consulting and copying data from computer systems,¹²² taking access to information by electronic means,¹²³ and seizing or sealing goods or computer systems.¹²⁴ When seizing computer systems (and thus data), the DPA is mindful of the potential impact this may have on the affected businesses and thus prefers to use this power not too frequently.¹²⁵

Furthermore, the DPA can also search information on publicly accessible websites, a power it may use to ‘scrape websites’ (including copying data).¹²⁶ The exact scope of this power remains however somewhat unclear and the DPA declared it does not cooperate with OSPs for this purpose.

Since June 2024, the DPA may also designate ‘experts’ (e.g. IT experts) for punctual help during the investigation,¹²⁷ but it has hardly used this power so far. The latter power may however be interesting to the extent it would be used to designate OSPs as ‘experts’.

In addition to those more general powers, the Inspection Service may also require the identification of the subscriber or habitual user of an electronic communication service or the communication means used (i.e. production of identification data).¹²⁸ This specific power can be used toward providers of electronic communications services operating in Belgium,¹²⁹ similar to the power granted to the FSMA (see 4.2.3.). The request for identification data must be based on a carefully reasoned decision of the Inspection Service, balancing the need for effective investigation with the principles of proportionality and privacy rights.¹³⁰ Although the DPA possesses this power, its use in practice is somewhat limited.

Next, it is highly noteworthy that the DPA concluded a cooperation agreement with DNS Belgium (i.e. a non-profit association whose mission consists in registering domain names, giving access to the internet and facilitating its access) in 2020.¹³¹ This agreement imposes upon DNS Belgium the obligation to provide the DPA all information that is useful for

¹²⁰ Article 66 § 1, 3° Act of 03.12.2017.

¹²¹ Article 66, § 1, 4° Act of 03.12.2017.

¹²² Article 66, § 1, 5° Act of 03.12.2017.

¹²³ Article 66 § 1, 6° Act of 03.12.2017.

¹²⁴ Article 66, § 1, 7° Act of 03.12.2017.

¹²⁵ Autorité de protection des données, *Rapport annuel 2020*, p. 44.

¹²⁶ Article 86 Act of 03.12.2017.

¹²⁷ Article 18/1, § 1 Act of 03.12.2017.

¹²⁸ Article 66 § 1, 8° Act of 03.12.2017.

¹²⁹ Article 73, § 2, para. 2 Act of 03.12.2017.

¹³⁰ Article 64, § 1 Act of 03.12.2017.

¹³¹ Available online at: <https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-dns-belgium-et-l-autorite-de-protection-des-donnees.pdf>.

its mission and to hand over documents and copies containing such information.¹³² If the information is part of a criminal investigation, the authorisation of the public prosecutor (or investigating judge in case of a judicial inquiry) is required. The cooperation agreement also creates a notice and action mechanism, which is useful for the DPA when seeking to detect infringements and identify the persons behind websites.¹³³ This mechanism gives the DPA the power to ask DNS Belgium to temporarily suspend a website, with users seeking access to the website being referred to a warning message on the DPA's website, or even to delete a website permanently.¹³⁴

The handling of electronic evidence plays a central role in modern data protection investigations. The Inspection Service takes special care to maintain the authenticity and traceability of electronic evidence, recognising the importance of preserving the integrity of such data throughout the investigative process. Typically, electronic evidence is collected on-site at the premises of the entity under investigation. This method allows the Inspection Service to ensure that the evidence remains intact and unaltered.

Non-cooperation with the DPA can be considered obstruction of justice and constitutes an offence.¹³⁵ In case of an expert designated by the DPA, he/she must also respect a duty of confidentiality, whose violation is punishable with a criminal fine.¹³⁶

4.3. Voluntary cooperation

Under Belgian law, cooperation with private actors in principle takes place within the boundaries set by the legal framework. Therefore, in general, voluntary cooperation between administrative authorities and private actors, including OSPs, is limited.¹³⁷ Most administrative authorities tend to rely on legal obligations and investigative powers to obtain information. The same also holds true for the collaboration and the exchange of information, which is usually based on formal agreements (see 5.1.).

While voluntary cooperation may occasionally occur, it is definitely not a prevailing practice among Belgian administrative authorities. For instance, the BCA, the NBB and the DPA strictly operate within formalized collaboration frameworks and within their legal powers. The NBB even openly questions the legality of data obtained on the basis of voluntary

¹³² Article 2 Cooperation agreement between DNS Belgium and the DPA.

¹³³ Article 2 Cooperation agreement between DNS Belgium and the DPA.

¹³⁴ Article 4 Cooperation agreement between DNS Belgium and the DPA.

¹³⁵ Article 222, 7° Act of 30.07.2018 on the Protection of Natural Persons Regarding the Processing of Personal Data (Act of 30.07.2018), Moniteur belge 05.09.2018.

¹³⁶ Article 224 Act of 30.07.2018.

¹³⁷ In criminal proceedings, voluntary cooperation is a bit more frequent. See Careel, Verbruggen, (n. 57), pp. 255-256.

cooperation. The FSMA may request voluntary cooperation from private actors for information or documents, but the success of these requests is contingent on the willingness of the actors involved.

As for the GACE, the position is that one may always ask, but without a legal framework, it is unlikely to obtain information or documents.

The VAT administration also relies on its legal powers. Since it rarely interacts with private actors who are not under investigation, the question of voluntary cooperation is considered not very relevant.

4.4. Concluding remarks

To effectively collect electronic evidence from OSPs, a clear and robust legislative framework is imperative. One of the primary challenges in this domain stems from the inherently territorial nature of legal powers, which contrasts sharply with the global business operations of many OSPs. These providers often reside in jurisdictions far removed from the location of the legal authorities seeking evidence, creating significant jurisdictional and procedural complexities.

Moreover, the collection of electronic evidence can be a very intrusive measure and must thus adhere to stringent procedural safeguards. These include ensuring that the collection process is necessary, proportionate, and authorized *ex ante* by a judicial authority (preferably a judge). Additionally, it is crucial for the protection of fundamental rights, such as privacy, data protection and fair trial rights, to secure the integrity of the evidence collected.

All in all, the foregoing analysis shows that the powers to obtain data from OSPs (or other private actors) in punitive administrative investigations are still relatively limited, though certainly not inexistent.

In certain sectors (e.g. customs and VAT), general powers could be used to obtain such data, but for the time being are not. In the three of the four sectors heavily influenced by EU law (financial markets, competition law and data protection law), the authorities have both general powers and specific powers enabling them to obtain data from certain OSPs. Yet, the use of these powers is still rather limited. This underutilisation may stem from a lack of awareness of the legal possibilities or from other significant challenges, such as jurisdictional issues. Unlike judicial authorities, the administrative authorities indeed stick to a strictly territorial application of their powers.

Access to content data in an administrative investigation is currently only possible through seizure, potentially in the context of a search of private premises, which normally concerns the suspect. Such data cannot be requested directly from OSPs by administrative authorities, unlike the more intrusive powers given to judicial authorities.

5. TRANSFER OF EVIDENCE BETWEEN PROCEEDINGS

5.1. Transfers of evidence between national proceedings

This section will discuss the legal possibilities and practice concerning the exchange of information between administrative authorities on the one hand (5.1.1.), and between administrative authorities and the public prosecutor's office on the other (5.1.2.). The second scenario is related to the question whether the administrative authorities can, or are obliged to, notify a criminal offence to the public prosecutor and transfer their case file to the latter, even if exchange of information may of course take place without shifting from administrative to criminal enforcement. Therefore, these rules will also be briefly presented, without aiming for an exhaustive analysis.

The legal landscape regarding the exchange of information is quite diverse. Yet, it should be pointed out from the outset that the rules (and practices) explained below are general ones. There are indeed no specific rules (or approaches) with regard to sharing data collected from OSPs or other private actors as third parties.

Moreover, exchange of *information* does not necessarily mean that the information exchanged will effectively be used as *evidence* by the other authority. That may be the case, but whether it is, it depends essentially on the decision of the authority receiving the information. That is why preference will be given to the more neutral term 'transfer of information' in the next few paragraphs.

In addition to the legal rules, cooperation and exchange of information are also facilitated by informal contacts, based on personal relationships or knowledge shared among individuals working within the administrative authority or the public prosecutor's office. The only exception seems to be the VAT administration, where the cooperation protocol is strictly observed.

5.1.1. Transfer of information between administrative authorities

As regards the collaboration between the competent administrative authorities in the respective Analysed Sectors and other administrative authorities, two main types of situations can be distinguished: 1) either the law regulates the possibility to cooperate and share information in a relatively detailed manner, or 2) the law only provides for a general possibility to cooperate, in which case the adoption of a more detailed cooperation agreement or 'protocol' may be needed. In certain sectors, these protocols are publicly available, in others they are not.

In the competition law field, collaboration between the BCA and other national administrative authorities requires a strict legal framework,

formalised through cooperation agreements enshrined in royal decrees governing the exchange of information.¹³⁸ The cooperation essentially concerns other supervisory or controlling administrative authorities active in the economic sector. In this sector, the adoption of a cooperation agreement by royal decree is considered necessary because BCA officials are bound by professional secrecy.¹³⁹ Violation of one's professional secrecy is a criminal offence.¹⁴⁰ Hence, they can only share confidential information obtained in the exercise of their functions if there is a legal basis for doing so, or put differently, if the law authorises the disclosure, hence providing a ground of justification.¹⁴¹

For example, a formal agreement exists between the BCA and the Belgian Institute for Postal Services and Telecommunications (IBPT),¹⁴² which functions well thanks to the established protocol, but also because the IBPT has enough staff to answer requests from the BCA. A similar agreement with the Commission for Electricity and Gas Regulation (CREG)¹⁴³ has proven to be less effective due to resource limitations on the CREG's side.¹⁴⁴ The BCA also sees potential benefits in establishing a similar agreement with the DPA, but no agreement has so far been adopted. Although the CEL provides for logistic or operational cooperation with the Ministry of Economy,¹⁴⁵ including the possibility to second staff of the Ministry to the BCA, the collaboration remains limited in practice. Occasionally, the BCA is invited to collaborate with regional authorities, such as the Flemish Regulator of the Electricity and Gas Market (VREG), but the absence of a formal legal framework hinders effective cooperation. Unlike the BCA, regional authorities tend to operate with more flexible frameworks for information exchange: the mere signature of a cooperation agreement suffices (i.e. without the adoption of a ministerial decree by the regional government). Overall, the BCA considers there is still considerable room for improving the cooperation with other administrative authorities.

Similarly, in the financial markets sector, the FSMA can share confidential information with other national (and international)

¹³⁸ Article IV.94 CEL.

¹³⁹ Article IV.32, § 1 CEL.

¹⁴⁰ Article XV.80, § 3 CEL.

¹⁴¹ This principle is also laid in Article 458 of the Criminal Code, which is the general criminal offence relating to the violation of a professional's obligation to secrecy.

¹⁴² Royal Decree of 08.05.2014 concerning the cooperation between the Belgian Institute for Postal Services and Telecommunications and the Belgian Competition Authority, *Moniteur belge* 14.07.2014.

¹⁴³ Royal Decree of 03.12.2017 concerning the cooperation between the Commission for the Regulation of Electricity and Gas and the Belgian Competition Authority, *Moniteur belge* 15.12.2017.

¹⁴⁴ Belgian Competition Authority, *Annual Report 2023, 2024*, p. 31.

¹⁴⁵ Article IV.16, § 4 and § 6 CEL.

administrative authorities based on Articles 74 and 75 of the Act of 2 August 2002. While Article 74 provides a legal exception to the obligation of professional secrecy by which the FSMA is bound,¹⁴⁶ Article 75 contains a long list of authorities with whom the FSMA can share information, including for instance the BCA, the DPA, the NBB, the Ministry of Economy and the Ministry of Finance. When the FSMA shares information with another authority, the latter is held by the same professional secrecy as the FSMA.¹⁴⁷

Obviously, not all exchange of information relates to a punitive context. In case of an investigation, however, information will typically be shared towards the conclusion of an investigation. For instance, when a legal entity regulated by the NBB is under investigation, the FSMA will inform the NBB thereof. Similarly, if there are anti-money laundering (AML) aspects involved, the FSMA will notify the Financial Intelligence Unit (FIU or '*CTIF*' in French).

While the Act of 2 August 2002 thus provides a direct legal basis (and does not require a royal decree to be adopted, contrary to the situation explained above for the BCA), the FSMA has adopted detailed cooperation agreements with a number of authorities mentioned by Article 75 of the Act of 2 August 2002. The FSMA is very transparent about the existence and content of these protocols (also called 'Memorandums of Understandings'): they are publicly available on the FSMA's website.¹⁴⁸ In particular, the FSMA has entered into more detailed cooperation agreements with, amongst others, the NBB, the CREG, the Ministry of Economy, the Ministry of Finance, the VAT administration and the FIU. In practice, cooperation runs smoothly and mainly concerns the FIU, the NBB, and the Ministry of Economy.

In the area of banking law, the legal framework is quite similar to the one explained for the FSMA. The Act of 22 February 1998 confirms the confidential nature of the information the NBB possesses – all officials of the NBB are bound by an obligation of professional secrecy¹⁴⁹ – and limits the use of this information to the purposes for which it has been collected.¹⁵⁰ But at the same time, the aforementioned Act also provides for several exceptions to the NBB's professional secrecy, particularly when it exercises its prudential supervisory mission and acts to prevent money laundering and financing of terrorism. Those legal exceptions enable the banking authority to share information with other national (and international) administrative authorities, such as the BCA, the FSMA, the Ministry of Economy, and the Ministry of

¹⁴⁶ Violation of that obligation is a criminal offence (Article 80, § 3 Act of 02.08.2002, referring to Article 458 Criminal Code).

¹⁴⁷ Article 75, § 4 Act of 02.08.2002.

¹⁴⁸ Available online at: <https://www.fsma.be/fr/accords-de-cooperation-nationaux>.

¹⁴⁹ Article 35, para. 1 Act of 22.02.1998.

¹⁵⁰ Article 36/12/4 Act of 22.02.1998.

Finance.¹⁵¹ In practice, the exchange of information is less common in the context of an investigation. Indeed, when information is exchanged, this usually concerns the NBB's supervisory tasks.

As far as data protection law is concerned, the Act of 3 December 2017 regulates in a general, much less detailed manner, the cooperation between the DPA and other national administrative authorities. First of all, it states that members of the DPA are bound by confidentiality and cannot share the information they have knowledge of in the exercise of their functions or missions.¹⁵² The DPA may however conclude cooperation agreements guaranteeing the confidentiality of this information when exchanged with third parties, including other administrative authorities. In this context, it is relevant to mention the cooperation agreement with DNS Belgium, adopted on 26 November 2020.¹⁵³ As explained (see 4.2.6.), this cooperation agreement creates a notice and action mechanism, which is very useful for the DPA when seeking to detect infringements and identify the persons behind websites, but it also ensures that the information by the DPA with DNS remains confidential.

Another protocol that has been adopted relates to the cooperation with the competent supervisory authorities referred to in Titles 2 and 3 of the Act of 30 July 2018.¹⁵⁴ This cooperation concerns, for instance, the handling of complaints affecting the competences of two or more supervisory authorities. To enable cooperation in this respect, the DPA and other supervisory authorities were required to conclude a cooperation protocol;¹⁵⁵ the latter was adopted in 2020.¹⁵⁶

Furthermore, Article 52 of the Act of 3 December 2017 sets that the DPA may be assisted by or act at the request of other public authorities responsible for enforcing other legislation,¹⁵⁷ without providing a list of authorities.

Conversely, Article 68, paragraph 1 of the Act of 3 December 2017 states that all state entities (including the public prosecutor's office) are required to provide to the Inspector General and inspectors, and at their request, all information they deem useful for monitoring compliance with the legislation they are responsible for and to produce, for their inspection, all

¹⁵¹ Article 36/13 and 36/14 Act of 22.02.1998.

¹⁵² Article 48, § 1 Act of 03.12.2017.

¹⁵³ Available online at: <https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-dns-belgium-et-l-autorite-de-protection-des-donnees.pdf>.

¹⁵⁴ Act of 30.07.2018 on the Protection of Natural Persons Regarding the Processing of Personal Data, Moniteur belge 05.09.2018.

¹⁵⁵ Article 54/1, § 2 Act of 03.12.2017.

¹⁵⁶ Available online at: <https://www.autoriteprotectiondonnees.be/citoyen/l-autorite/autres-autorites>.

¹⁵⁷ Article 52 Act of 03.12.2017.

information and provide copies thereof in any form. For instance, if the DPA would receive a complaint about the use of surveillance cameras, it may contact the police and ask for useful information to conduct its investigation. That said, if the requested information is part of an ongoing criminal investigation, it can only be communicated with the prior authorisation of the public prosecutor or investigating judge who is in charge of the investigation.¹⁵⁸ In practice, the public prosecutor or investigating judge sometimes gives a conditional authorisation, setting certain limits to the use of the exchanged information.

Some similarities can be found in the field of VAT law. Cooperation of the VAT administration with other administrative authorities is regulated by Article 93bis of the VAT Code, stating that the officials of the VAT administration are bound by an obligation of professional secrecy. They are however allowed to share information with other administrative authorities (as well as with the public prosecutor's office and the courts) to the extent that the information is necessary for ensuring the exercise of the other authority's legal missions.¹⁵⁹ The latter requirement is obviously important. Authorities receiving information from the VAT administration are then deemed bound by the same duty of professional secrecy and they have to respect the principle of speciality, meaning they cannot use the information outside the legal framework and missions for which the information has been shared.¹⁶⁰ Exchange of information may take place at the request of the other administration or at the initiative of the VAT administration holding the information, and vice versa. In practice, the exchange of information seems to be based on a protocol, which is not publicly available. Cooperation is considered smooth and frequent, especially with other tax authorities (including the GACE) and the Ministry of Economy.

Lastly, under customs law, the dynamic is rather different. As indicated, the GACE has prosecutorial powers and thus is an administrative authority wearing a (semi-)judicial hat. This translates into a different legal framework when it comes to the exchange of information. In accordance with Article 210, § 1 of the General Act of 18 July 1977, all state entities and public institutions (including the public prosecutor's office) are required, when asked by a GACE official, to communicate without charge all documents and information in their possession. When this information concerns a criminal investigation, an explicit authorisation of the public prosecutor is required.¹⁶¹ Moreover, within the Ministry of Finance, all tax authorities (including the GACE, but also the VAT administration) are obliged to share all relevant

¹⁵⁸ Article 68 Act of 03.12.2017.

¹⁵⁹ Article 93bis, para. 1 VAT Code.

¹⁶⁰ Article 93bis, para. 2 VAT Code.

¹⁶¹ Article 210, § 1, para. 3 General Act of 18.07.1977.

information which their colleagues to establish and collect taxes.¹⁶² Furthermore, in addition to sharing information, other state authorities (including the police) may actively intervene in certain investigation measures conducted by the GACE (e.g. search of private premises and seizure).¹⁶³ In some cases, they may also be required to assist and protect GACE officials in the exercise of their missions.¹⁶⁴

To conclude, the (cooperation and) exchange of information between administrative authorities always requires a legal basis under Belgian law. In several sectors, the possibility of exchanging information is explicitly regulated as an exception to the obligation to professional secrecy or as a form of joint exercise of this obligation. In practice, cooperation seems to be smooth, especially between authorities whose missions are related to one another (e.g. FSMA and NBB, VAT and GACE). Authorities seem to struggle a bit more to obtain information from other national authorities that are not a 'natural partner' (i.e. an authority with a similar mission). Finally, smooth exchange of information also requires that the requested authority has sufficient resources to follow up on the requests for information (e.g. BCA and its cooperation with the Ministry of Economy).

5.1.2. Transfer of information between administrative authorities and the public prosecutor's office

5.1.2.1. Introduction

Exchanging information between administrative authorities is one thing; exchanging information between administrative authorities and the public prosecutor's office is yet another as the procedural safeguards applicable under administrative law (even when punitive in nature) are not the same as under criminal law. Hence, the exchange of information between administrative authorities and the public prosecutor's office may entail a risk of abuse, particularly when information would be gathered under legislation setting lower standards and subsequently used as evidence in criminal proceedings.

As indicated in the introduction of 5.1., the exchange of information between administrative authorities and the public prosecutor's office also connects to the question whether administrative authorities have an obligation to notify a criminal offence to the public prosecutor's office and the (legal) criteria or (factual) circumstances that may justify a switch from administrative to criminal enforcement. These related questions will only be

¹⁶² Article 210, § 3 General Act of 18.07.1977.

¹⁶³ Article 197 General Act of 18.07.1977.

¹⁶⁴ Article 327 General Act of 18.07.1977.

dealt with briefly, as a detailed analysis exceeds the objectives of the present chapter.

5.1.2.2. Taking the public prosecutor's office perspective

Generally speaking, the public prosecutor's office has a right and duty of information.¹⁶⁵ As such, it can obtain information from any other Belgian authority, including authorities conducting an administrative investigation, through a formal request for information. This request and the subsequent answer of the requested authorities will be included in the criminal case file.

Moreover, Article 29, § 1 of the CCP entails an obligation for any authority in Belgium to immediately inform the public prosecutor's office of a criminal offence (more precisely, a '*crime*' or a '*délit*')¹⁶⁶ that has come to its knowledge in the exercise of its functions, and to transmit all relevant information and documents to the public prosecutor's office.

Of course, these are general rules; the law may provide for exceptions or exemptions, as will be discussed below.

Furthermore, if the public prosecutor takes over an investigation initiated by an administrative authority, the evidence collected during the administrative investigation will in most cases simply be included in the criminal case file, notwithstanding the fact that the evidence was collected with lower procedural safeguards.

However, the reverse scenario – where an administrative authority seeks information from a criminal investigation – is less straightforward and strongly varies from one sector to another, as will be explained below.

5.1.2.3. Similar rules for exchange of information with administrative and judicial authorities...

To start with, as can be concluded from the analysis in section 5.1.1., the legal framework on exchange of information sometimes regulates the exchange of information between an administrative authority and the public prosecutor's office in (almost) the same way as the exchange of information between administrative authorities.

For instance, in the field of data protection law and customs law, the legislation obliges all state entities, including the public prosecutor's office, to share useful information with the DPA¹⁶⁷ and the GACE.¹⁶⁸ Access to

¹⁶⁵ Article 28ter CCP.

¹⁶⁶ The obligation does not extend to the least serious category of offences, i.e. '*contraventions*'.

¹⁶⁷ Article 68 Act of 03.12.2017.

¹⁶⁸ Article 210, § 1 General Act of 18.07.1977.

information contained in a criminal case file requires the authorisation of the public prosecutor (or, in case of a judicial inquiry, the investigating judge).

Under VAT law, the tax administration may share information with the public prosecutor's office to the extent that the information is necessary for the latter's mission.¹⁶⁹

5.1.2.4. ... Yet, special rules regarding the notification of offences and to conditions for switching to criminal enforcement

The law however strictly regulates the procedure to be followed to notify a tax offence to the public prosecutor's office. This procedure also applies to VAT offences. Officials of the GTA and the SIS can only notify a VAT offence to the public prosecutor's office upon the authorisation of the general counsel whom they are subordinated to.¹⁷⁰ Without such formal notification, the public prosecutor cannot legally start a criminal investigation.

In addition, in case of serious indications of serious tax fraud (*'indices sérieux de fraude fiscale grave'*), the law provides for a formal consultation procedure between the tax authorities and the public prosecutor's office (involving also the police). Based on this consultation, the public prosecutor's office will decide whether to prosecute. In the affirmative, it must inform the tax administration of its decision, at the latest three months after receiving the notification.¹⁷¹

In practice, it is mainly the SIS that notifies offences to the public prosecutor. This is not entirely surprising considering the SIS mainly deals with fraud cases, not less serious VAT infringements (see 2.). When notifying an offence to the public prosecutor's office, the VAT administration will usually already have conducted its own investigation – in other words, the notification does not necessarily happen at the very start. For instance, the VAT administration may decide to wait until it has reached the limits of its own powers before notifying the offence to the public prosecutor. Considering the VAT administration has quite extensive powers, it is quite likely that the public prosecutor will be required to open a judicial inquiry¹⁷² soon after deciding to take over the case from the administration. If the VAT offence is however connected to other offences that do not belong to the

¹⁶⁹ Article 93bis, para. 1 VAT Code.

¹⁷⁰ Article 29, § 2 CCP.

¹⁷¹ Article 29, § 3 CCP.

¹⁷² Under Belgian criminal procedure, a judicial inquiry is necessary for the most intrusive investigation measures, such as an arrest warrant or the secret search of an information system (Article 28septies CCP).

competence of the VAT administration (e.g. forgery or fraudulent bankruptcy), the VAT administration will likely ask for a consultation earlier on in the investigation. In such case, the public prosecutor may decide to take over the entire investigation or only the offences that are not tax offences.

If the public prosecutor decides to take the case, the VAT administration must in principle hand over the entire case file. The public prosecutor indeed has the power to seize the administrative case file. This way, all evidence collected by the VAT administration will directly end up in the criminal case file and can be legally used as evidence in the criminal proceedings. Later access to the criminal case file by the VAT administration requires the authorisation of the public prosecutor, who can of course refuse to grant such access.

Even if the GACE is also part of the tax administration, the foregoing notification procedure and consultation mechanism does *not* apply to customs offences. Informal consultation mechanisms may, however, exist in certain judicial districts. This difference can be explained by the hybrid nature of the GACE's investigations (see 2.) and the prosecutorial powers the GACE is vested with. The GACE will indeed prosecute customs offences itself in criminal court, with a limited role for the public prosecutor (see 2.).¹⁷³ In case the customs offences are connected to other offences, the GACE and the public prosecutor can prosecute together, each for the offences that belong to their respective material competence.¹⁷⁴

Furthermore, it is worth pointing out that the GACE has an obligation to cooperate with the EPPO.¹⁷⁵ The relation with the EPPO is complex and quite delicate, both at the level of the law and in practice. Whether the current approach is compatible with the EPPO Regulation is highly uncertain.¹⁷⁶ While a further analysis of this relation exceeds the objectives of this chapter, it is important to highlight that GACE officials, when conducting an investigation under the authority of the EPPO, may still use their own extensive investigation powers as defined by the General Act of 18 July 1977,

¹⁷³ Article 281, §§ 1-2 General Act of 18.07.1977. For a more detailed analysis, see Franssen, Claes, (n. 3), pp. 181-190.

¹⁷⁴ Article 281, § 3 General Act of 18.07.1977. In practice, though, such joint prosecutions are fairly rare.

¹⁷⁵ Article 285/1 ff. General Act of 18.07.1977.

¹⁷⁶ See e.g. Tipik and Spark Legal and Policy Consulting, *Compliance assessment of measures adopted by the Member States to adapt their systems to Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')*, Study carried out for the European Commission (JUST/2022/PR/JCOO/CRIM/0004), 2023, pp. 32-33 and 71-72.

offering less procedural safeguards than the CCP.¹⁷⁷ GACE officials with the status of ‘officer of judicial police’ can, in addition, use the more intrusive powers of the CCP (see 4.2.1.).

In the area of data protection law, there is a legal procedure facilitating the exchange of information between the DPA and the public prosecutor's office, which is closely connected to the possibility to switch from administrative to criminal enforcement.

According to that procedure, both the Inspector General and the Litigation Chamber have the power to refer the file to the public prosecutor. The former can do so when they wrap up the investigation.¹⁷⁸ The latter has this possibility (i) either before deciding whether the case is ready for a decision on the merits,¹⁷⁹ i.e. when the case is brought before the Chamber by the First-Line Service upon a complaint, by a party exercising the right to legal remedy against a measure by the Inspection Service or by the Inspection Service at the end the investigation,¹⁸⁰ or (ii) when the Litigation Chamber considers the case is ready for a decision on the merits.¹⁸¹

If the Inspector General's report to the Litigation Chamber mentions findings of violations of legislation other than that concerning the protection of personal data, the Litigation Chamber must provide a copy of these findings to the public prosecutor.¹⁸²

Upon referral, the public prosecutor shall inform the DPA of the follow-up given to the file.¹⁸³

Next, if the public prosecutor decides not to initiate criminal proceedings, propose an amicable settlement, or initiate a mediation procedure within the meaning of Article 216ter of the CCP, or when the public prosecutor has not made a decision within six months of receiving the file, the DPA determines whether the administrative proceedings should be resumed.¹⁸⁴

¹⁷⁷ For further analysis, see A. L. Claes, V. Franssen, ‘When EPPO Meets Customs: A Clash of Enforcement Strategies and Procedural Safeguards’, Jean Monnet Network on EU Law Enforcement (EULEN), Working Paper Series, vol. 09-22, 2022.

¹⁷⁸ Article 91, § 2 Act of 03.12.2017.

¹⁷⁹ Article 95, § 1, 7° Act of 03.12.2017.

¹⁸⁰ Article 92 Act of 03.12.2017.

¹⁸¹ Article 100, § 1, 15° Act of 03.12.2017.

¹⁸² Article 97 Act of 03.12.2017.

¹⁸³ Articles 95, § 1, 7° and 100, § 1, 15° Act of 03.12.2017.

¹⁸⁴ Article 95, § 3 and Article 100, § 2 Act of 03.12.2017.

5.1.2.5. Separate rules for the cooperation with the public prosecutor

Unlike the three sectors dealt with above, the sectorial legal framework on financial markets and banking law contains specific rules on the cooperation with the public prosecutor's office, i.e. rules that differ from the ones applicable to the cooperation with other administrative authorities. At the same time, this framework also regulates whether offences must or may be notified to the public prosecutor's office.

In the field of financial markets law, the FSMA and the public prosecutor's office may establish a protocol governing the working relationship between the FSMA and the public prosecutor's office in cases involving acts for which the legislation provides for both the possibility of an administrative fine and the possibility of criminal sanctions.¹⁸⁵

Despite the current absence of such protocol, collaboration between the FSMA and the public prosecutor's office is considered swift. When a grievance is notified by the Management Committee to the potential wrongdoer and that such grievance also constitutes a criminal offence, the Management Committee informs the public prosecutor's office thereof. If the public prosecutor's office then decides to prosecute, it immediately informs the FSMA. The public prosecutor's office may provide the FSMA, either *ex officio* or at the request of the latter, with a copy of any document relating to the subsequent criminal investigation.¹⁸⁶

In practice, the notification by the Management Committee to the public prosecutor's office does not prevent the continuation of the case at the administrative level, unless the public prosecutor's office indicates that it is prosecuting the case. In such instances, the matter is left to the public prosecutor's office and the FSMA pauses its work.

There are no criteria established by law or by protocol to determine whether the public prosecutor will take up a case. In general, the public prosecutor's office will take on cases of particular severity or those involving public personalities or attracting media coverage.

Interestingly, the FSMA may ask the public prosecutor's office to collect evidence on its behalf.¹⁸⁷ In practice, that possibility is rarely used by the FSMA as it considers having sufficient powers itself.

Conversely, judicial authorities can ask the FSMA any information or documents relevant to the investigation of types of market abuse that are criminally punishable. In practice, the public prosecutor's office or the

¹⁸⁵ Article 73 Act of 02.08.2002.

¹⁸⁶ Article 71, § 5 Act of 02.08.2002.

¹⁸⁷ Article 35 Act of 02.08.2002.

investigating judge exercises this prerogative to take advantage of the expertise and resources of the FSMA. Indeed, the FSMA has dedicated technicians, economists and legal advisors specialized in market abuse. Moreover, as a dedicated authority, it is more familiar with certain notions than the public prosecutor's office. For instance, using this prerogative, judicial authorities may also seek legal advice from the FSMA on whether the suspects had access to so-called 'privileged information'.¹⁸⁸

A quite different scenario can be found in banking law.

First of all, it is important to note that the NBB is exempted by law¹⁸⁹ from the obligation laid down in Article 29 of the CCP to report offences to the public prosecutor's office. Instead, the NBB has a legal possibility to report offences.¹⁹⁰ The reason for the exemption is that the notification of an offence to the public prosecutor's office may have far-reaching consequences for the stability of the banking system (e.g. a rush on the bank). The NBB will thus carefully balance the different interests at stake before reporting an offence. If it does, it may publish this decision.¹⁹¹ Conversely, under the Act of 25 April 2014 on the control of credit institutions,¹⁹² there is an obligation for the judicial authorities to inform the NBB of any information regarding an infringement that belongs to the latter's competence.

Second, beyond the notification of offences, in some specific instances collaboration (and thus exchange of information) with the public prosecutor's office may take place. The NBB is, for instance, allowed by law to provide testimony in court.¹⁹³

5.1.2.6. Lack of formal rules

Finally, competition law stands out by the fact that there is, at present, no express legal basis enabling cooperation between the BCA and the public prosecutor's office, notwithstanding the fact that the bid rigging clearly is a serious criminal offence¹⁹⁴ and the BCA officials can establish criminal offences.¹⁹⁵ In practice, there is some informal cooperation, but it depends on the willingness to cooperate of the individual public prosecutor in the case at hand. Moreover, the cooperation is limited to purely procedural information

¹⁸⁸ Article 40bis Act of 02.08.2002.

¹⁸⁹ Article 35, § 1, para. 2 Act of 22.02.1998.

¹⁹⁰ Article 35, § 2, para. 1, 2° Act of 22.02.1998.

¹⁹¹ Article 35, § 2, para. 2 Act of 22.02.1998.

¹⁹² Act of 25.04.2014 on the Status and Supervision of Credit Institutions, Moniteur belge 07.05.2014.

¹⁹³ Article 35, § 1, para. 1 Act of 22.02.1998.

¹⁹⁴ Article 314 Criminal Code. In addition, the CEL also contains some other criminal offences (Article XV.80 CEL).

¹⁹⁵ Article IV.40/1, para. 1 CEL.

(e.g. on the existence of an investigation) in an attempt to avoid double proceedings. In contrast, there is no sharing or exchange of information in concrete cases. To illustrate this, the BCA stated that its requests for access to the case file of the public prosecutor are always refused, and vice versa. The BCA regrets this lack of cooperation and argues in favour of adopting a legal basis to that end. For instance, it could be useful to have access to the electronic communications data gathered by the public prosecutor as the latter has more experience in collecting such data.

5.2. Transfers of evidence between foreign and national proceedings

5.2.1. Introduction

The rules on international cooperation provided by national law are rather limited, as most international cooperation is based on EU legislation (e.g. GDPR or MAR) or conventions (e.g. Naples II Convention¹⁹⁶ in the customs field). With third countries, the possibility of cooperation depends on the existence of bilateral or multilateral treaties (ensuring reciprocity). It would however take us too far to list and examine those. Moreover, from the interviews with the respective national competent authorities in the Analysed Sectors, it is quite clear that most international cooperation concerns EU partners.

As far as there are specific national rules on transfer of evidence between national and foreign authorities, they are, however, not specific to data collected from OSPs or other private actors. Therefore, their added value for this research is limited.

In the following lines, a short account of the national rules will be given per sector, along with the practice of the respective competent national authorities. The intensity or frequency of cross-border cooperation (including the exchange of information) varies considerably from one sector to another.

5.2.2. National rules and practices

Under customs law, the law states that the GACE is authorised to provide all information, certificates, records and other documents to competent authorities in foreign countries for the purposes to prevent, detect and sanction offences against the laws and regulations on import or export. Such exchange of information is only possible on the basis of reciprocity.¹⁹⁷ The reverse situation (i.e. whether the GACE can use information it receives from foreign authorities) is not explicitly addressed, but the requirement of

¹⁹⁶ Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations, OJ C 24/2, 1999.

¹⁹⁷ Article 325 General Act of 18.07.1977.

reciprocity suggests this is allowed. In addition, Article 164 of the General Act of 18 July 1977 sets that GACE officials may consider as valid the signs or stamps put on the goods (*'marques de contrôle apposées (...) sur des marchandises'*) or vehicles by a foreign tax authority, certifying the control of such goods or vehicles.

While much of the international cooperation in customs matters takes place on the basis of the Naples II Convention, it is however noteworthy that the GACE, as a hybrid authority with prosecutorial powers, can also use the European investigation order (EIO) to collect evidence in another EU Member State.¹⁹⁸ In accordance with Article 24, § 5 of the Belgian EIO Act,¹⁹⁹ it can indeed issue an EIO relating to matters for which it is exclusively competent. That said, before transmitting the EIO to the foreign executing authority, the GACE must have it validated by an investigating judge. This validation consists in a simple legality check. As regards incoming requests, the GACE is the competent authority to execute those relating to its exclusive competence.²⁰⁰ Incoming requests may be sent directly to the GACE or to the public prosecutor's office,²⁰¹ which will transmit them to the GACE.²⁰²

Next, the VAT Code states that the Belgian VAT authorities may exchange with authorities from other EU Member States all information that is relevant to determine the VAT due within the EU.²⁰³ This information can be used on the same as information gathered by the Belgian VAT administration, in line with EU law.²⁰⁴ Conversely, information gathered by the Belgian VAT administration for tax authorities in other EU Member States must respect the same rules as information gathered for national cases and can only be transmitted for the purposes defined by EU law.²⁰⁵ It is also allowed to conclude an agreement with another EU Member State enabling a foreign tax official to gather information in Belgium, and vice versa.²⁰⁶ Information collected abroad on the basis of such agreement can be legally used in a Belgian VAT investigation, on the same conditions as information collected in Belgium.²⁰⁷

In practice, international cooperation in the field of VAT law is greatly facilitated by the existence of (for sure still imperfect) EU systems platforms where data is exchanged automatically.

¹⁹⁸ For more details, see Franssen, Claes, (n. 3), pp. 212-215.

¹⁹⁹ Act of 22.05.2017 on the European Investigation Order, *Moniteur belge* 23.05.2017.

²⁰⁰ Article 4, 6° EIO Act.

²⁰¹ Article 4, § 1, para. 2 EIO Act.

²⁰² Article 14, §§ 2-3 EIO Act.

²⁰³ Article 93terdecies, para. 1 VAT Code.

²⁰⁴ Article 93terdecies, para. 2 VAT Code.

²⁰⁵ Article 93terdecies, para. 3 VAT Code.

²⁰⁶ Article 93terdecies, paras 4-5 VAT Code.

²⁰⁷ Article 93terdecies, para. 5 VAT Code.

In the field of competition law, the BCA collaborates with the national competition authorities (NCAs) of other EU Member States and with the European Commission.

In this respect, Belgian law tasks the BCA with carrying out assistance, verification, or other missions toward undertakings and individuals at the request of the NCA of another EU Member State or at the request of the European Commission.²⁰⁸ In such context, the BCA is authorised to communicate to the European Commission and to NCAs any factual or legal elements. On the other hand, the BCA may use information obtained from the European Commission or foreign NCAs as evidence.²⁰⁹

In practice, though, the exchange of information between NCAs is sometimes hampered by national procedural rules and, with regard to individuals, by the rules regarding professional secrecy. Therefore, the ‘free flow of information’ as enabled by Regulation 1/2003²¹⁰ largely remains a fiction in the BCA’s view.

With respect to concrete cases, the BCA has the possibility to ask for the assistance of experts from another NCA, for instance, during dawn raids. While some practical examples of such cooperation exist, there is a lack of uniformity in procedures and legal frameworks governing such cooperation.

NCAs also exchange best practices within the European Competition Network (ECN), but despite the existence of recommendations from the ECN²¹¹ and working groups on best practices, there is no formal standardised procedure at the EU level that establishes such cooperation.

Finally, when it comes to sharing concrete tools (e.g. forensic software for data collection and analysis), there is still a lot of room for improvement. More cooperation between the European Commission and the NCAs would be welcome, especially in light of new technological challenges.

As regards financial markets, the FSMA engages in collaboration with the competent authorities of other EU Member States that exercise one or more comparable competencies, alongside European Securities and Markets Authority (ESMA).²¹² Concerning market abuse, the MAR mandates this cooperation, which is directly applicable within each Member State.²¹³

²⁰⁸ Article IV.77 CEL.

²⁰⁹ Article IV.78 CEL.

²¹⁰ Article 12(1) and recital 16 Council Regulation (EC) 1/2003 of 16.12.2002 on the implementation of the rules on competition laid down in Article 81 and 82 of the Treaty, OJ L1/1, 16.12.2003.

²¹¹ See online: https://competition-policy.ec.europa.eu/system/files/2021-07/ecn_recommendation_09122013_digital_evidence_en_0.pdf.

²¹² Article 24 MAR.

²¹³ Article 25 MAR.

Additionally, the FSMA has concluded numerous bilateral and multilateral cooperation agreements with its counterparts.²¹⁴ At the EU level, ESMA facilitates cooperation through Memorandums of Understanding, while internationally, cooperation agreements are provided by IOSCO (i.e. the International Organisation of Securities Commissions).

Nevertheless, for the FSMA, personal contacts remain crucial in ensuring effective collaboration. The latter is of paramount importance, particularly in matters of market abuse, which often entail extraneous elements.

In the area of banking law, cooperation mainly concerns the European Central Bank. Such cooperation may concern general information, but also concrete cases. The European Central Bank may also ask national authorities to prosecute. In general, this cooperation is smooth, facilitated by informal contacts too. The NBB however rarely needs international cooperation for its investigations; such cooperation is mainly useful for the NBB's supervisory tasks.

Finally, with respect to data protection law, the Belgian law states that the DPA may cooperate with any data protection authority in another state using its powers as defined by the GDPR (for the EU context) or national law.²¹⁵ This collaboration may include: (i) establishing centres of expertise, (ii) exchanging information, (iii) providing mutual assistance in performing control measures, and (iv) sharing human and financial resources.²¹⁶ This collaboration can be formalized through cooperation agreements.²¹⁷

5.3. Admissibility of evidence

In this final Section, we will focus on the delicate question whether the collected evidence is admissible. Roughly speaking, the admissibility of evidence in Belgian punitive administrative proceedings follows a consistent approach, even if there is no general legal framework applicable to all Analysed Sectors (see 3.). Moreover, the rules are not in any way tailored to the specific question of data collected from OSPs or other private actors.

First of all, the law in most cases does not state which types of evidence are admissible, or if it does, it covers a wide range of evidence. In principle, the admissibility of evidence is thus free. In this respect, punitive

²¹⁴ Available online at: <https://www.fsma.be/fr/accords-de-cooperation-internationaux>.

²¹⁵ Article 55, § 1 Act of 03.12.2017.

²¹⁶ Article 55, § 2, para. 1 Act of 03.12.2017.

²¹⁷ Article 55, § 2, para. 2 Act of 03.12.2017.

administrative procedure resembles criminal procedure, where the same principle²¹⁸ applies, even if it is not expressly provided by law.²¹⁹

Second, with respect to illegally obtained evidence, administrative authorities typically state that they apply the same rules as those provided by law for criminal proceedings, even if, interestingly, the law or case law does not always explicitly recognize the applicability of those rules.

The rules on the admissibility of illegally obtained evidence in criminal proceedings can be found in Article 32 of the Preliminary Title to the CCP, which are a codification of the so-called ‘Antigone’ case law of the Belgian Supreme Court (*Cour de cassation*). According to that legal provision, illegally obtained evidence is inadmissible and must be excluded in only three scenarios: (i) when the evidence has been collected in violation of a formal legal requirement whose non-respect is sanctioned with nullity, (ii) when the irregularity committed undermines the reliability of the evidence, or (iii) when the use of the evidence is contrary to the right to a fair trial. In practice, the exclusion of illegally obtained evidence is rather rare in criminal proceedings. With regard to the first scenario, it should be pointed out that there are only a handful of rules of criminal procedure whose compliance is prescribed under penalty of nullity. The second scenario could be useful with respect to digital evidence, for instance when the chain of custody or the integrity of the data cannot be properly verified. But in practice the courts rarely apply this scenario. Concerning the third and last scenario, the case law is equally strict. For instance, with respect to the use of illegally retained electronic communications data in criminal proceedings, the *Cour de cassation* confirmed that a violation of the rights to privacy and the protection of personal data, as laid down in Article 8 ECHR and Articles 7 and 8 of the Charter of Fundamental Rights of the EU (Charter), does not hamper the exercise of the rights of defence nor amounts to a violation of the right to a fair trial.²²⁰ As a result, the exclusion of illegally obtained evidence is rather exceptional in criminal proceedings.²²¹

Turning now to punitive administrative proceedings, the application by analogy of the rules applicable in criminal proceedings is in some cases based

²¹⁸ For sure, there are a few exceptions to this principle, but they are not directly relevant for the subject of this chapter.

²¹⁹ For an overview of the rules applicable in criminal procedure, see e.g. M. A. Beernaert, D. Vandermeersch, M. Giacometti, *Droit de la procédure pénale*, La Charte, 2025, pp. 1510–1514.

²²⁰ See e.g. Cass., 24.05.2020, No P.19.0571.N; Cass., 19.04.2016, No P.15.1639.N. See also Careel, Verbruggen, (n. 57), pp. 224–226.

²²¹ V. Franssen, C. Van de Heyning, ‘Belgium’s New Data Retention Legislation: Third Time Lucky, or Three Strikes and You’re Out?’ in: E. Kosta, I. Kamara (eds), *Data Retention in Europe and Beyond*, Oxford University Press, 2025, p. 264.

on an explicit legal basis in the sectorial legal framework; in other cases, it follows from legal practice.

For instance, in the field of competition law, Article IV.40/6 CEL expressly outlines the rules governing the admissibility of evidence since March 2022.²²² That Article states that evidence admissible before the BCA includes documents, oral statements, electronic messages, recordings, and any other item containing information, regardless of its form and medium. Hence, the range of admissible evidence is broad and definitely provides the necessary flexibility to encompass digital evidence.

As regards the admissibility of illegally obtained evidence, Article IV.40/6 CEL sets forward the same three scenarios as the ones laid down in Article 32 of the Preliminary Title of the CCP. In other words, the collected evidence, regardless of its form, is admissible unless it has been obtained in violation of formal conditions sanctioned with nullity, affects the reliability of the evidence, or contravenes the right to a fair trial.

Under VAT law, the administration is authorized to prove an infringement ‘in accordance with the rules and by any means allowed under the general rules of law, including by testimony and presumptions (...) and by means of records drafted by the official of the Federal Public Service Finance’²²³ (i.e. the Ministry of Finance). The VAT administration may also designate experts to evaluate the value of goods and services subject to VAT.²²⁴ Once again, the range of admissible evidence is broad and does not seem to raise any problems for digital evidence.

Next, as regards the admissibility of illegally obtained evidence, the VAT Code does not contain any explicit rules. According to the *Cour de cassation*, the use of such evidence must thus be evaluated in light of the principles of good administration and the right to a fair trial.²²⁵ Therefore, still according to the Court, illegally obtained evidence does not have to be excluded unless it has been obtained in a manner so contrary to what is expected from an administration that it must be considered inadmissible, or that its use would put at risk the right to a fair trial. When making his/her assessment, the judge may take into account, for instance, the purely formal nature of the procedural irregularity, the impact of the irregularity on the right protected by the legal norm that was violated, the intentional or unintentional nature of the illegality and the circumstance that the seriousness of the infringement exceeds considerably the illegality committed. Interestingly, the

²²² This provision was inserted by the Act of 28.02.2022 transposing Directive (EU) 2019/1 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, Moniteur belge 07.03.2022.

²²³ Article 59, § 1, para. 1 VAT Code.

²²⁴ Article 59, § 2, para. 1 VAT Code.

²²⁵ See e.g. Cass., 18.01.2018, no. F.16.0031.N; Cass., 29.01.2021, no. F.17.0016.N.

latter criteria correspond almost exactly to the ones put forward by the *Cour de cassation* in criminal matters, when applying Article 32 of the Preliminary Title to the CCP.²²⁶ Hence, even if on its face the regime applicable to VAT seems to differ, in practice the assessment is made on the basis of the same criteria. This undoubtedly explains why legal scholars²²⁷ and the VAT administration simply refer to the ‘Antigone’ case law when asked about the rules applicable to illegally obtained evidence in VAT proceedings.

In practice, the admissibility of illegally obtained evidence is regularly challenged in VAT cases. An interesting case relates to the questions discussed above, on the transfer of evidence between different proceedings, involving also a cross-border dimension. In the case at hand, a judicial inquiry regarding VAT carousel fraud had been opened in Belgium after a formal complaint by the VAT administration. In the context of that criminal investigation, a rogatory commission was executed in Luxembourg on the basis of the Benelux Mutual Legal Assistance (MLA) Treaty of 27 June 1967. In accordance with of Article 20 of that Treaty, a search and seizure order were conducted at a Luxembourgish bank. During the search, the bank director was interrogated by the Luxembourgish investigating judge, in the presence of his Belgian colleague, and handed over bank documents concerning the suspects, which were added in annex to the interview record. According to paragraph 2 of Article 20 of the Benelux MLA Treaty, the seized documents could only be transferred to the Belgian judicial authorities upon the approval of the pre-trial tribunal (*‘Chambre du conseil’*) of the location of the bank. Yet, in the case at hand, this approval was not requested. Notwithstanding this, the documents were included in the Belgian criminal case file. Subsequently, the Belgian VAT administration requested and obtained access to the criminal case file. It could thus make a copy of the bank documents and use them for the administrative proceedings. The use of the documents was later contested by the accused at trial, yet the court of appeal considered the documents were admissible, arguing that it was quite unlikely that the pre-trial tribunal in Luxembourg would have refused the Belgian authorities to take the collected documents home to use them as evidence, and considering that the irregularity was ‘insufficiently proportionate’ to the gravity of the offences committed. The judgment of the court of appeal was challenged before the *Cour de cassation*, which decided to refer a preliminary question to the European Court of Justice (ECJ).²²⁸ In particular, the ECJ was asked whether the right

²²⁶ For a more detailed analysis of the criteria observed in criminal matters, see Beernaert, Vandermeersch, Giacometti, (n. 219), pp. 1538-1543.

²²⁷ See e.g. V. De Brabanter, G. Vael, Y. Zheng, ‘Les conséquences pratiques des mécanismes de coopération internationale en matière de procédure fiscale belge: état des lieux’, *Revue Générale de Fiscalité et de Comptabilité Pratique*, 2019, no. 5, p. 33.

²²⁸ Cass., 18.06.2018, no. F.17.0016.N.

to a fair trial (Art. 47 Charter) should be interpreted in such manner that evidence obtained in violation of the right to private life (Art. 7 Charter) must be excluded. The ECJ, however, considered the preliminary ruling was inadmissible as there are no common rules at EU level on the admissibility of evidence in VAT matters.²²⁹ Eventually the *Cour de cassation* decided that the court of appeal had legally decided to not exclude the illegally obtained evidence in the VAT proceedings.²³⁰ In other words, despite the illegality committed, the evidence obtained in the cross-border criminal proceedings could be used in the Belgian administrative proceedings.

Under customs law, the rules on admissibility in criminal proceedings clearly apply, considering the GACE has prosecutorial powers (see 2.). In the absence of special rules in the General Act of 18 July 1977, the rules on nullity as defined by Article 32 of the Preliminary Title of the CCP are thus applicable to illegally obtained evidence in customs proceedings. In a recent judgment, a first instance tribunal went even a step further.²³¹ According to the tribunal, the reliability of the evidence was fundamentally flawed because the GACE had focused its investigation on one suspect without searching for other, potentially exculpatory evidence. Any evidence that suggested the suspect was not guilty had been discarded from the administrative case file and were not mentioned in the report concluding the customs investigation. The trial court therefore ruled the GACE had conducted the investigation in a partial manner and had thus violated the right to a fair trial (Art. 6 ECHR), resulting in the inadmissibility of the prosecution.

Finally, in the other three Analysed Sectors (banking law, financial markets law and data protection law), the rules on admissibility of evidence are not expressly provided by law, but the interviewed authorities all confirmed that they apply the rules on criminal procedure by analogy. Challenges to the admissibility of evidence appear to be relatively rare in practice, as demonstrated by the low number of disputes in administrative punitive decisions. For instance, in the financial markets sector, the FSMA declared it seldom faces disputes over evidence admissibility, possibly due to the well-defined legal framework on FSMA investigations and the regulatory authority's solid reputation. In case of doubt, the Investigation and Prosecution Unit of the FSMA will decide itself to exclude the evidence to avoid litigation later in the process. Interestingly, this cautious approach sometimes leads to a stricter application of the rules on laid down in Article 32 of the Preliminary Title of the CCP. For instance, in the aftermath of the

²²⁹ ECJ, *IN and JM v. Belgische Staat*, 24.10.2019, Joined Cases C-469/18 and C-470/18.

²³⁰ Cass., 29.01.2021, no. F.17.0016.N.

²³¹ Corr. Liège, 12.12.2024, *Journal des tribunaux de Liège, Mons et Bruxelles*, 2025, vol. 10, p. 424.

ECJ's case law on the Belgian data retention legislation,²³² the FSMA concluded that it could no longer use electronic communications data that had been retained in violation of EU law, whereas the *Cour de cassation* decided otherwise in criminal proceedings, arguing the right to a fair trial had not been violated (see above).²³³

6. CONCLUSION

If one thing, this chapter has revealed that the Belgian legal framework regarding the gathering of electronic evidence in the six Analysed Sectors is highly fragmented and lacks consistency. Moreover, considering the technicality of the sectors and the varying institutional setting, a thorough understanding of the topic is only possible by also examining the practice of the competent authorities. Depending on the sector, one and the same issue can be dealt with very differently and thus one should always carefully analyse the applicable legal framework and practice before jumping to conclusions.

If consistency is hard to find, the Analysed Sectors do have a few key points in common: the gathering of electronic evidence is still largely underregulated (with a few exceptions) and the cooperation with OPSs remains rather limited, even where specific powers in this regard exist. Therefore, more comparison with the powers under criminal procedure, where the cooperation with OSPs is already extensively regulated, as well as the exchange of best practices with the police and judicial authorities, which have years of experience in gathering electronic evidence from third parties, would definitely be beneficial for the future of electronic evidence gathering in punitive administrative proceedings.

²³² ECJ, *La Quadrature du Net and others*, 06.10.2020, Joined Cases C-511/18, C-512/18 and C-520/18).

²³³ See e.g. Cass., 11.01.2022, no. P.21.1245.N; Cass., 25.01.2022, no. P.21.1353.N, 2022, vol. 3, *Tijdschrift voor Strafrecht*, p. 160 (case comment by C. Van de Heyning); Cass., 29.03.2022, no. P.21.1422.N; Cass., 29.03.2022, no. P.22.0078.N.

ANNEX 1 – LIST OF INTERVIEWS

Sector	Competent Authority	Name	Function	Date of interview
Customs Law	GACE	Michaël Moustier	Head of Investigation Unit, Liège	22.03.2024
	Private practice	Raphaël Van de Sande	Consultant, previously GACE Operational Unit, Liège	16.01.2024
VAT Law	GTA	Marie-Christine Jans	General Counsel	17.01.2024
	GTA	Benoît Van Vyve	General Counsel	02.07.2024
	GTA	Thomas Keutgen	VAT official (' <i>Attaché</i> ')	02.07.2024
	GTA	Marjorie Hagelsteens	VAT official (' <i>Attachée</i> ')	02.07.2024
	SIS	<i>Yannic Hulot</i>	<i>Head of SIS</i>	<i>No agreement for interview</i>
Financial Markets Law	FSMA	Isabelle Legrand	Auditor, Head of Enforcement	25.01.2024
Banking Law	NBB	Ann Dirkx	Auditor	02.07.2024
	NBB	Yannick Fadeur	Enforcement Unit Rapporteur	02.07.2024
Competition Law	BCA	Damien Gérard	Auditor General	17.01.2024
Data Protection Law	DPA	Peter Van den Eynde	Inspector General	12.01.2024
Public Prosecutor's Office	PPO Walloon Brabant	Magali Raes	PPO's economic and financial crime Division	22.11.2024; 25.01.2024

5. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN FINLAND

J. RIEKKINEN

1. COMPETENT AUTHORITIES IN SELECTED AREAS OF PUNITIVE ADMINISTRATIVE ENFORCEMENT

In Finland, various administrative authorities are empowered to impose punitive administrative sanctions. In the selected areas, the relevant authorities are the Finnish Customs (*Tulli*), the Tax Administration (*Verohallinto*), the Financial Supervisory Authority (*Finanssivalvonta*, FIN-FSA) and the Data Protection Ombudsman (*tietosuojavaltuutettu*). In the field of competition law, the competent administrative agency – the Finnish Competition and Consumer Authority (*Kilpailu- ja kuluttajavirasto*, FCCA) – has no power to impose such penalties independently but may make proposals concerning punitive sanctions to the Market Court (*markkinaoikeus*).

In the area of customs enforcement, the Finnish Customs has both administrative and criminal enforcement competences. Firstly, it is the authority with the competence to issue punitive administrative sanctions under Chapter 14 of the Customs Act.^{1,2} These include punitive customs duty

¹ *Tullilaki* 304/2016. Finnish parliamentary acts and other legislative texts are officially available in Finnish and in Swedish. Some unofficial translations for parliamentary acts and decrees are available in Finlex, an online database of legislative and judicial information. See Finlex, ‘Translations of Finnish acts and decrees’ 2024 (last updated), online <https://www.finlex.fi/en/laki/kaannokset/>. However, for many acts discussed in this report, no translation is available. English translations of legal texts and their titles in this report are therefore mostly the author’s own. The original Finnish titles of the referenced acts and certain specific terms used in legislation are provided for clarity.

² Additionally, the Border Guard and the Police have limited customs duties. See Border Guard Act (*rajavartiolaitoslaki*, 578/2005), s 24; Police Act (*poliisilaki*, 872/2011), c 2 s 21; Customs Act ss 3–5. The cooperation between these authorities is further regulated in the Act on Cooperation between the Police, the Customs and the Border Guard (*laki poliisin, Tullin ja Rajavartiolaitoksen yhteistoiminnasta*, 687/2009).

increase (*tullinkorotus*)³ and two other types of monetary sanctions, which can be both be translated as administrative fines or penalty payments (*virhemaksu* and *seuraamusmaksu*).⁴ Secondly, the Customs have the competence to prevent, expose and investigate customs offences under the Act on Crime Prevention in the Customs⁵ and the Criminal Investigation Act.^{6,7} As a criminal investigation authority, the Customs may use most of the investigative powers defined in the Coercive Measures Act,⁸ whereas its powers for crime prevention are regulated in the aforementioned Act on Crime Prevention in the Customs. These acts regulate numerous investigatory powers that enable access to electronic evidence held by suspects and third parties, such as search of data contained in a device, telecommunications interception, traffic data monitoring, and production of subscriber information.⁹ These provisions are not applicable in punitive administrative proceedings.

³ A punitive customs duty increase can be imposed in connection with the decision regarding customs duty, or in a separate decision under the Act on Punitive Tax Increases and Punitive Customs Duty Increases Imposed by Separate Decisions (*laki erillisellä päätöksellä määrättävästä veron- tai tullinkorotuksesta*, 781/2013). As the title of the Act suggests, the same applies to punitive tax increases.

⁴ Customs Act, ss 95, 96 and 99a, respectively. In the Customs Act, *seuraamusmaksu* specifically refers to an administrative sanction for infringements of Article 3(1) of the Regulation (EU) 2019/880 of the European Parliament and of the Council of 17 April 2019 on the introduction and the import of cultural goods, whereas *virhemaksu* can be imposed for a wider range of violations. In Finnish legislative terminology, *seuraamusmaksu* is typically a punitive administrative sanction for more severe violations and omissions, whereas penalties for lesser infractions may be called *virhemaksu* or *rikemaksu*. In the case of the Customs Act, however, there is no clear difference in the severity of the two sanctions, and the maximum amount of *virhemaksu* is actually higher for certain violations (the ranges are 50–15.000 € for *virhemaksu* and 500–10.000 € for *seuraamusmaksu*). Although in English, the term ‘administrative fine’ is also commonly used, in Finnish the word *sakko* (‘fine’) should be reserved for criminal sanctions. The use of these terms has not always been consistent in domestic legislation, and as no official English translations for parliamentary acts exist, translations in different sources discussing Finnish law may be inconsistent. The legislative terminology of the EU may create further confusion. See Finlex, ‘Lainkirjoittajan opas’ 2014 (last updated 2024), online <https://lainkirjoittaja.finlex.fi/>, 12.10.2 (Hallinnollisen sanktion määrittely) and O. Mäenpää, K. Kiiski, R. Lindberg, et al., *Rangaistusluonteisia hallinnollisia seuraamuksia koskevan sääntelyn kehittäminen. Työryhmän mietintö. Mietintöjä ja lausuntoja 52/2018*, Helsinki, Ministry of Justice, 2018, pp. 20–21.

⁵ *Laki rikostorjunnasta Tullissa*, 623/2015.

⁶ *Esitutkintalaki*, 805/2011.

⁷ On the duty of the Customs to notify the Police and transfers of investigations to the Police, see Act on Crime Prevention in the Customs, c 2 ss 2–3.

⁸ *Pakkokeinolaki*, 806/2011.

⁹ Generally on the Coercive Measures Act and electronic evidence, see J. Riekkinen, ‘Evidence of Cybercrime and Coercive Measures in Finland’ *Digital Evidence and Electronic Signature Law Review*, 2016, vol. 13, pp. 50, 55–66, DOI:10.14296/deeslr.v13i0.2296.

The competent tax enforcement authority is the Tax Administration. The tasks and organisation of the Tax Administration are generally regulated in the Act on the Tax Administration.¹⁰ In relation to value-added tax (VAT) violations, the Tax Administration may impose punitive tax increases (*veronkorotus*), late-filing fees (*myöhästymismaksu*) and negligence penalties (*laiminlyöntimaksu*) under the Act on the Assessment Procedure of Self-assessed Taxes,¹¹ Chapter 7. Similar sanctions are made possible for certain other taxes in the Act on the Assessment Procedure.¹² The latter Act is also relevant in proceedings related to VAT and other self-assessed taxes (i.e., taxes that the taxpayer must calculate, file, and pay themselves) due to numerous references to its provisions, notably including provisions concerning third party obligations to provide information.

The Financial Supervisory Authority has the competence to investigate violations of various legal obligations relating to banking and financial markets, and to impose punitive administrative sanctions for these violations. The primary legislative instrument regulating the tasks and organisation of the FIN-FSA is the Act on the Financial Supervisory Authority (FSA Act).¹³ However, the material scope of the supervisory competence of the FIN-FSA is broad and defined by dozens of legislative instruments. In addition to national parliamentary acts, these include a number of legislative instruments of the European Union (EU).¹⁴ Several of these – e.g., the Market Abuse Regulation (MAR)¹⁵ and the Benchmark Regulation¹⁶ – require the competent national supervisory authorities to have the power to issue administrative sanctions. In domestic law, the FIN-FSA's primary investigative powers and competence to impose administrative sanctions are regulated in the FSA Act, Chapters 3 and 4, respectively. Chapter 4 defines two types of monetary sanctions, the more lenient administrative fine

¹⁰ *Laki Verohallinnosta*, 503/2010.

¹¹ *Laki oma-aloitteisten verojen verotusmenettelystä*, 768/2016.

¹² *Laki verotusmenettelystä*, 1558/1995.

¹³ *Laki Finanssivalvonnasta*, 878/2008.

¹⁴ See FSA Act, ss 50a–50w and the referred EU instruments.

¹⁵ Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.

¹⁶ Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014.

(*rikemaksu*)¹⁷ and the more severe penalty payment (*seuraamusmaksu*).¹⁸ Chapter 4 further allows the FIN-FSA to issue a public warning (*julkinen varoitus*).¹⁹ In addition, the FIN-FSA has some competence to impose administrative sanctions as defined in anti-money laundering and consumer protection laws,²⁰ which also contain some additional provisions on investigatory powers.²¹ Decisions on all administrative sanctions are made by the Board of the FIN-FSA.²²

As mentioned, the administrative authority that is tasked with enforcing competition law is the FCCA. The tasks and organisation of the FCCA are outlined in the Act on the FCCA (FCCA Act).²³ Unlike the other authorities discussed in this report, the FCCA does not have the competence to issue punitive administrative sanctions independently. Instead, Section 12 of the Competition Act²⁴ states that penalty payments (*seuraamusmaksu*) for restrictions of competition are imposed by the Market Court upon the proposal of the FCCA. Since 2021, penalty payments can also be imposed in the same order for violations of procedural obligations relating to inspections

¹⁷ An administrative fine is imposed regarding certain violations specified in FSA Act, s 38, and amounts to 5.000–100.000 €, or 500–10.000 € for a natural person.

¹⁸ A penalty payment under FSA Act, s 40 can amount up to 10.000.000 € or 10% (or in some cases, even 15.000.000 € or 15%) of the legal person's yearly turnover. See FSA Act, ss 41 and 41a on the maximum amounts in different situations. – The distinction between *rikemaksu* and *seuraamusmaksu* corresponds to the general usage of these Finnish terms, as stated in Mäenpää, Kiiski, Lindberg, et al., (n. 4), p. 21. The respective English translations mentioned in the text are used in the unofficial translation of the FSA Act, as well as on the FIN-FSA website. However, in other contexts, such as data protection law, the English term corresponding to (*hallinnollinen*) *seuraamusmaksu* (which can be a very severe sanction) is 'administrative fine'.

¹⁹ According to FSA Act, s 39, a public warning can be imposed for financial market violations other than those defined in ss 38 and 40, which concern administrative fines and penalty payments, respectively. These provisions contain numerous references to other legislation. See in particular Securities Markets Act (*arvopaperimarkkinalaki*, 746/2012), c 15 ss 1 and 2. The latter further refers to, e.g., several MAR provisions, therefore fulfilling the requirements of MAR, Article 30 concerning the power of the competent national authorities to impose administrative sanctions.

²⁰ See Act on Detecting and Preventing Money Laundering and Terrorist Financing (*laki rahanpesun ja terrorismin rahoittamisen estämisestä*, 444/2017, AML Act), c 8; Act on Certain Powers of the Consumer Protection Authorities (*laki kuluttajansuojaviranomaisten eräistä toimivaltuuksista*, 566/2020, CPCPA Act), ss 5, 13, 15 and 16. Similar to the FSA Act, sanctions available under the AML Act include administrative fines, penalty payments and public warnings, whereas CPCPA Act regulates penalty payments (*seuraamusmaksu*) only.

²¹ See AML Act, c 7; CPCPA Act, c 2.

²² FSA Act, s 10(1)(5).

²³ *Laki Kilpailu- ja kuluttajavirastosta*, 661/2012.

²⁴ *Kilpailulaki*, 948/2011.

and cooperation during investigations.²⁵ Chapter 5 of the Competition Act contains procedural rules that apply to FCCA investigations, and the Administrative Judicial Procedure Act²⁶ is applicable to the proceedings and decision-making in the Market Court.²⁷

The national supervisory authority required by Article 51 of the General Data Protection Regulation (GDPR)²⁸ is the Data Protection Ombudsman. The organisation of the Office of the Data Protection Ombudsman and complementary rules on investigative powers and decision-making relating to administrative sanctions under the GDPR are found in the Data Protection Act.²⁹ According to Section 24 of this Act, administrative fines as regulated in GDPR, Article 83 (*hallinnollinen seuraamusmaksu*) are imposed by a collegial body for sanctions (Sanctions Board, *seuraamuskollegio*), which is composed of the Data Protection Ombudsman and the two Deputy Data Protection Ombudsmen.³⁰ Beyond the GDPR, the Data Protection

²⁵ See Competition Act, s 37a (amendment 546/2021, which entered into force on 24.6.2021). In May 2024, the FCCA submitted its first proposal for a penalty payment based on this provision to the Market Court (Proposal of 22.5.2024, KKV/376/14.00.00/2023 (Attendo Oyj)).

²⁶ *Laki oikeudenkäynnistä hallintoasioissa*, 808/2019.

²⁷ Beyond competition law enforcement, the FCCA has supervisory tasks, investigatory powers, and the power to propose administrative sanctions relating to public procurement and – as its name suggests – consumer protection, which are not further discussed in this report. Generally, see FCCA Act, s 2 (and in relation to certain tasks relating to EU legislation, ss 7b–7f); Act on Public Procurement and Concession Contracts (*laki julkisista hankinnoista ja käyttöoikeussopimuksista*, 1397/2016), in particular c 15 and 16; Consumer Protection Act (*kuluttajansuojalaki*, 38/1978); CPCPA Act, in particular c 2 and 3. The FCCA is the national competent authority in relation to Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). As the European Commission is the sole authority empowered to enforce Digital Markets Act, the role of the FCCA is limited to information exchange and assisting the Commission, and it may not impose or propose sanctions on its own.

²⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

²⁹ *Tietosuojalaki*, 1050/2018.

³⁰ In Finland, it was considered inappropriate to grant an individual person the power to decide on administrative fines under the GDPR, as these may be very significant sanctions. As a result, a collegial model was adopted for these decisions, even though the Data Protection Ombudsman may make most other administrative decisions related to GDPR enforcement on their own. Generally, the Deputy Data Protection Ombudsmen have the same powers as the Data Protection Ombudsman in the performance of their tasks (Data Protection Act, s 16).

Ombudsman has further supervisory tasks and duties in other areas of enforcement that fall outside the scope of this chapter.³¹

Besides the Customs, none of the other authorities mentioned above have parallel criminal investigation tasks or duties in addition to their administrative enforcement competence.³²

2. PUNITIVE ADMINISTRATIVE PROCEEDINGS: GENERAL FRAMEWORK

While the first punitive administrative sanctions were introduced to the Finnish legislation in the 1970s, their use has increased in large part, but not exclusively, due to the requirements of EU law during the last two decades.³³ Increasingly, punitive administrative sanctions have been used as a substitute to criminal punishment for lesser violations and omissions, and in sectors vulnerable to the grey economy.³⁴ They are considered a lighter and more flexible regulatory means than criminal punishment, although it is noted that from the perspective of the European Charter of Human Rights (ECHR),

³¹ These include the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, and Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). The Data Protection Ombudsman (or rather, the Sanctions Board) may impose administrative sanctions for some violations under the national complementary Act on the Supervision of Online Intermediary Services (*laki verkon välityspalvelujen valvonnasta*, 18/2024), ss 3, 16(2) and 20(5). However, the designated Digital Services Coordinator (under Article 49) is the Finnish Transport and Communications Agency (Traficom).

³² However, even though the Data Protection Ombudsman is not tasked with investigating criminal offences, Criminal Code (*rikoslaki*, 39/1889), Chapter 38, Section 10(3) provides that the prosecutor must consult them before bringing charges for certain offences targeting personal data filing systems, and the court must give them an opportunity to be heard in such cases.

³³ See L. Hankila, V. Lankinen and A. Nilsson, *Administrativa sanktionsavgifter. En nordisk komparativ studie*, Copenhagen, Nordic Council of Ministers, 2018, pp. 157–185.

³⁴ Finnish authorities define grey economy (or ‘shadow economy’) as activity in which ‘statutory obligations are neglected, for example, to avoid paying taxes, or statutory pension insurance, accident insurance or unemployment insurance contributions or fees collected by the Finnish Customs, or to receive unjustified refunds’ or ‘other statutory obligations are neglected to receive financial benefits’. Grey economy & economic crime website (Tax Administration), ‘Definitions of the grey economy and economic crime’ 2021, online <https://www.vero.fi/en/grey-economy-crime/scope/definition/>.

punitive administrative proceedings are subject to the same procedural rights and due process requirements that apply to criminal proceedings.³⁵

In addition to human rights, it is important to note the role of fundamental rights enshrined in the Constitution of Finland.³⁶ While certain procedural rules or investigative measures might be acceptable from the perspective of the ECHR and other human rights obligations, they might not be permitted under domestic constitutional law doctrine, as it may entail a higher level of protection in relation to various rights of the individual.³⁷ For instance, while the Constitution of Finland specifically allows for limitations to the secrecy of communications in the investigation of criminal offences and in certain other situations, it does not permit similar limitations in punitive administrative proceedings.³⁸ In practice, this precludes administrative authorities from using certain covert measures such as telecommunications interception and traffic data monitoring, although such measures may be available to their foreign counterparts.³⁹ These measures can only be carried out by criminal justice and intelligence authorities,⁴⁰ and the uses and transfers of resulting information are also limited.⁴¹ Another constitutional issue to consider is the principle of legality, enshrined in Section 2(3) of the Constitution, which requires the exercise of public powers to be based on the law, and the law to be strictly observed in all public activity.

³⁵ See Finlex, ‘Lainkirjoittajan opas’ 2014 (last updated 2024), online <https://lainkirjoittaja.finlex.fi/>, 12.10 (Hallinnollisten sanktioiden sääntelyperiaatteet); O. Mäenpää, *Hallinto-oikeus*, Helsinki, Alma Talent, 3rd edition, 2023 (online version), online <https://verkkokirjahylly.almatalent.fi/teos/BAXBXATIBIEE>, II.4., Hallinnolliset seuraamukset ja hallintopakko, Hallinnolliset sanktiot. From a Nordic perspective, see also Hankila, Lankinen, Nilsson, (n. 33), pp. 16–17.

³⁶ *Suomen perustuslaki*, 731/1999.

³⁷ This doctrine is largely influenced by the praxis of the parliamentary Constitutional Law Committee, which issues statements on the constitutionality of bills during parliamentary proceedings.

³⁸ Constitution of Finland, s 10(4) (which was amended by Act 817/2018 to permit new intelligence legislation): ‘Limitations of the secrecy of communications may be imposed by an Act if they are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, during deprivation of liberty, and for the purpose of obtaining information on military activities or other such activities that pose a serious threat to national security.’ Cf. ECHR, Article 8(2).

³⁹ See also section 3.1.3 of this report.

⁴⁰ The Police, the Customs and the Border Guard may perform traffic data monitoring in order to prevent, expose or investigate criminal offences. See Coercive Measures Act, c 10 ss 6–9; Police Act, c 5 ss 8–10; Act on Crime Prevention in the Customs, c 3 ss 4–6; Act on Crime Prevention by the Border Guard (*laki rikostorjunnasta Rajavartiolaitoksessa*, 108/2018), ss 16–18. Further, traffic data monitoring is possible for civilian and military intelligence purposes under Police Act, c 5a s 7 and Act on Military Intelligence (*laki sotilastiedustelusta*, 590/2019), ss 37–38. In most cases, traffic data monitoring requires a court warrant.

⁴¹ See section 4.1 of this report.

Among other things, this necessitates that the investigatory powers of administrative authorities are regulated on the level of parliamentary acts with sufficient precision. The Constitution also contains provisions on the right to an effective remedy, fair trial and good administration, as well as the duty of the public authorities to guarantee the observance of fundamental and human rights.

In Finland, there is currently no comprehensive parliamentary act or other legislative instrument that specifically governs punitive administrative proceedings. General legislation on punitive administrative proceedings was recently considered by a government-appointed working group, which ultimately deemed it unnecessary at this time.⁴² In addition, this working group formulated some regulatory principles concerning punitive administrative sanctions.⁴³

At the level of parliamentary acts, the most important part of the relevant general legal framework is arguably the Administrative Procedure Act,⁴⁴ which lays down provisions on the general principles of good administration and the procedure applicable in all administrative matters, including administrative investigations and decision-making regarding punitive administrative sanctions. However, when a punitive administrative sanction is imposed by a court instead of an administrative authority, the Administrative Judicial Procedure Act applies to the court proceedings and decision-making.⁴⁵ This is the case in competition law enforcement, where administrative sanctions are laid down by the Market Court after a proposal from the FCCA.⁴⁶

Still, it is important to note that the Administrative Procedure Act does not establish a comprehensive framework on punitive administrative sanctions. Authorities may not impose punitive administrative sanctions without a specific legal basis in other legislation, which establishes the competence of the authority in question to issue punitive administrative sanctions for specified violations of legal obligations and defines the types of sanctions that are available.⁴⁷ Typically, such legislation also contains various procedural rules.

⁴² Mäenpää, Kiiski, Lindberg, et al., (n. 4), pp. 12–16.

⁴³ In summary, see *ibid.*, pp. 49–54.

⁴⁴ *Hallintolaki*, 434/2003.

⁴⁵ See Mäenpää, Kiiski, Lindberg, et al., (n. 4), pp. 42–43.

⁴⁶ In the Nordic countries, the concept of administrative sanctions usually covers sanctions laid down by a court after a proposal from an administrative authority. On the definition of the concept from a Nordic perspective, See Hankila, Lankinen, Nilsson, (n. 33), pp. 23–38.

⁴⁷ According to Administrative Procedure Act, s 67, '[a]n authority may reinforce a prohibition, obligation or requirement imposed by it by way of a notice of coercive fine, notice of enforced compliance or notice of enforced suspension, or another administrative consequence, as separately provided.'

Chapter 2 of the Administrative Procedure Act establishes the general principles of good administration, such as equal treatment, impartiality and proportionality.⁴⁸ These must be taken into consideration in all activities of public authorities.⁴⁹ More specifically concerning administrative proceedings, general provisions on examining a matter and on hearing the views of the parties are contained in Chapter 6.⁵⁰ Generally, authorities must ensure that matters are sufficiently and appropriately examined by acquiring the information and evidence necessary for a decision to be made.⁵¹ They must also provide all parties with an opportunity to be heard.⁵² Requests for statements or evidence must specify the particular points to be covered,⁵³ and time-limits set for submitting statements or evidence must be sufficient ‘in view of the nature of the matter’.⁵⁴ The Chapter further contains provisions on site visits, inspections and taking of oral evidence. All of these are *lex generalis* norms that apply in punitive administrative investigations, unless conflicting or more precise rules are found elsewhere in legislation. Notably, the provisions concerning requests for evidence (which are typically sent to the parties, but can also be sent to other authorities, external experts, or any other persons or entities) do not grant an authority the competence to obligate private third parties to provide information during administrative proceedings, and ignoring such a request does not carry legal consequences unless a specific legal obligation is established elsewhere in the law.⁵⁵

In contrast, during judicial proceedings in both administrative and general courts, everyone has a general obligation to produce documents and objects as evidence. Under the Administrative Judicial Procedure Act, the court – such as the Market Court, when deciding on a penalty payment proposal by the FCCA – may order any private party, including third parties, to produce documents (including digital data) and objects to the court, if they can be presumed to have significance as evidence. A coercive fine may be imposed to enforce compliance with the order.⁵⁶ The obligation to produce evidence is limited by the provisions on the rights and obligations not to

⁴⁸ See Administrative Procedure Act, s 6; see also ss 7–10.

⁴⁹ See Mäenpää, (n. 35), II.3., Hallinnon oikeusperiaatteet.

⁵⁰ Further, the status of parties in an administrative matter and some general rights of the parties are established in Administrative Procedure Act, c 3.

⁵¹ Administrative Procedure Act, s 31(1).

⁵² Administrative Procedure Act, s 34.

⁵³ Administrative Procedure Act, s 32.

⁵⁴ Administrative Procedure Act, s 33.

⁵⁵ See Mäenpää, (n. 35), III.7., Viranomaisen selvityspyyntö.

⁵⁶ Administrative Judicial Procedure Act, s 51(1); see also s 38, defining the general obligations.

testify in court.⁵⁷ Before a production order is given, the party in question must be given an opportunity to be heard.⁵⁸

Additional provisions on investigative powers and rights to obtain (or obligations to provide) information are found in sector-specific legislation and legislation concerning different administrative authorities, which have the status of *lex specialis* in relation to the Administrative Procedure Act. In Finland, punitive administrative sanctions have been considered more suitable for situations where the non-compliance with legal obligations is relatively easy to prove and specific investigative powers are not required.⁵⁹ Perhaps as a consequence, many acts that allow for an administrative authority to impose punitive administrative sanctions therefore contain limited, if any, rules on specific investigative powers. Further, as the Finnish legislation generally adheres strongly to the principle of technology neutrality, such provisions usually make no distinction between electronic evidence and other types of information or means of evidence. Additionally, it should be noted that these provisions are usually not limited exclusively to the context of ongoing punitive administrative proceedings that may lead to the imposition of an administrative sanction but cover access to information needed for any tasks and duties of the authority in question.

A commonly available enforcement measure for various obligations to provide information is a coercive fine (*uhkasakko*) imposed by the administrative authority (or, in judicial proceedings, by the court).⁶⁰ The coercive fine may be set as a lump sum or as a periodic penalty payment, in which case the payable amount increases periodically while the obligation has not been fulfilled. In the event of non-compliance, typically the same authority (or court) may order the payment of the fine. General norms concerning coercive fines are found in the Act on Coercive Fines.⁶¹ Like punitive administrative sanctions, a coercive fine may only be imposed when

⁵⁷ See Administrative Judicial Procedure Act, ss 69–71. Concerning proceedings in the general courts, see Code of Judicial Procedure (*oikeudenkäymiskaari*, 4/1734), c 17 ss 10–23. The Administrative Judicial Procedure Act contains several references to the Code of Judicial Procedure.

⁵⁸ Administrative Judicial Procedure Act, s 51(2) and Code of Judicial Procedure, c 17, s 40(2).

⁵⁹ Mäenpää, Kiiski, Lindberg, et al., (n. 4), pp. 25–26; Finlex, ‘Lainkirjoittajan opas’ 2014 (last updated 2024), online <https://lainkirjoittaja.finlex.fi/>, 12.10.3 (Hallinnollisen sanktion käyttöala sekä suhde hallinnollisiin ja rikosoikeudellisiin seuraamuksiin).

⁶⁰ In this report, the term ‘coercive fine’ is used in reference to *uhkasakko*, whereas unofficial translations of Finnish acts at Finlex generally utilise the term ‘conditional fine’. Concerning different obligations to provide information that can be enforced with a coercive fine, see K. Määttä, *Uhkasakko sekä teettämis- ja keskeyttämisuhka – Uhkasakkolain välilliset hallintopakkokeinot*, Helsinki, Edita, 2021, pp. 99–104. A coercive fine can also be imposed to enforce various other kinds of obligations, requests, and prohibitions.

⁶¹ *Uhkasakkolaki*, 1113/1990.

specifically so stated elsewhere in legislation,⁶² and sector-specific legislation may contain rules that have precedence over the *lex generalis* rules.⁶³

The Administrative Procedure Act further contains general rules on the form and contents of administrative decisions (Chapter 7), procedure for requesting administrative review (Chapter 7a)⁶⁴ and administrative complaints (Chapter 8a).⁶⁵ Appeals against administrative decisions are generally regulated in the Administrative Judicial Procedure Act, in particular Chapters 2 and 3. As a main rule, decisions by administrative authorities can be appealed to an Administrative Court. Administrative Court decisions may be further appealed to the Supreme Administrative Court, although in most cases such an appeal requires the granting of a leave to appeal.⁶⁶ Again, provisions in sector-specific legislation have precedence over the *lex generalis* norms. With some minor exceptions, decisions through which an administrative authority imposes punitive administrative sanctions can be appealed under the general rules. The same applies to certain decisions relating to obligations to provide information, in particular decisions concerning the imposition and payment of coercive fines as an enforcement measure.⁶⁷ In contrast, requests for evidence as such are typically not considered to constitute appealable decisions, as discussed later in connection with the sectorial frameworks.⁶⁸

Notably, the Administrative Procedure Act and other general legislation do not contain any specific remedies against evidence-gathering from third parties during administrative investigations. The general legislation also does not regulate *ex ante* notifications to the suspected entity concerning requests for evidence sent to third parties. However, as parties have a general right to be heard in regard to claims and evidence which may influence the final administrative decision in the matter,⁶⁹ evidence cannot be gathered from third parties without eventually notifying the suspected entity. This means that

⁶² Act on Coercive Fines, s 4; Administrative Procedure Act, s 67.

⁶³ Act on Coercive Fines, s 3.

⁶⁴ An appeal may need to be preceded by a request for an administrative review, if so specifically stated in law.

⁶⁵ Administrative complaints can be filed by anyone against authorities, persons employed by them and other entities performing public administrative duties concerning unlawful conduct or failure to fulfil an obligation. As a result, the overseeing authority may issue administrative guidance or initiate other legal proceedings, which may in turn lead to sanctions such as a warning, dismissal or criminal penalties. However, the overseeing authority may not repeal or modify an administrative decision. Complaints concerning an authority's unlawful activities may also be filed with the Chancellor of Justice and the Parliamentary Ombudsman.

⁶⁶ See Administrative Judicial Procedure Act, ss 107 and 110–111.

⁶⁷ See Act on Coercive Fines, s 24.

⁶⁸ See section 3.1 of this report.

⁶⁹ See Administrative Procedure Act, s 34.

they can present their view on the admissibility of any evidence before an administrative sanction is imposed, or before a proposal on a sanction is submitted to the court.⁷⁰ It is also worth noting that parties in any administrative matters generally have broad access rights to documents held by public authorities that may be relevant in their case.⁷¹

3. PUNITIVE ADMINISTRATIVE PROCEEDINGS: SECTORIAL FRAMEWORK

3.1. Requests for data to online service providers

3.1.1. Customs enforcement

As regards administrative proceedings, the Customs Act does not contain any specific provisions on electronic evidence. However, it does contain general, technology neutral provisions on obligations to provide information to the Customs. While Section 102(1) of the Customs Act concerns the person affected by the administrative investigation or any other official tasks by the Customs excluding criminal investigation or border investigation, Section 102(2) obligates all third parties that hold information that is needed for another person's customs taxation, or appeals thereof, to provide it to the Customs on request by a given time-limit. If a person has the right not to testify in regard to some information, the obligation does not apply to this information. However, the third party may not refuse to give information regarding the financial situation of the involved person. In addition to the national legislation, provision of information to the Customs is regulated in Article 15 of the Union Customs Code (UCC).⁷²

Although third parties' possible rights not to testify are acknowledged in Section 102(2), the text of the provision does not differentiate between any specific data categories. However, aforementioned limitations in the national constitutional doctrine, in particular concerning confidential communications, mean that the general provision cannot be interpreted to cover access to any and all data possessed by all kinds of OSPs. In particular, requests for information cannot in practice constitute a covert measure that corresponds to telecommunications interception or traffic data monitoring. It is less clear whether Section 102(2) might be interpreted to permit requests concerning subscriber identity information. In this consideration, it is noteworthy that in the Act on Crime Prevention in the Customs – applicable

⁷⁰ In competition law enforcement, the suspected entity specifically has the right to be heard before the proposal for a penalty payment is made by the FCCA (Competition Act, s 38(4)).

⁷¹ See Act on the Openness of Government Activities (*laki viranomaisten toiminnan julkisuudesta*, 621/1999), s 11 and the reference in Administrative Procedure Act, s 24(2).

⁷² Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code.

to the Customs as a criminal justice authority – the section that regulates the right of the Customs to receive information from third parties contains a separate subsection specifically regarding subscriber information, in addition to the more general provision resembling Customs Act, Section 102(2).⁷³

The Customs Act and the UCC do not contain any specific rules on the technical aspects of data transfers to the Customs beyond the UCC, Article 15(1) requirement that documents and information shall be provided ‘in an appropriate form’. According to Customs Act, Section 103, the person providing information to or assisting the Customs based on UCC, Article 15 or Customs Act, Section 102 must do so at their own expense. The time-limits for providing the information are not defined in the law, and may be specified by the Customs.⁷⁴

To enforce compliance with the obligation to provide information, the Customs may impose a coercive fine on the person bound by Section 102(2) of the Customs Act or UCC, Article 15, as provided in Section 104 of the Customs Act. The privilege against self-incrimination is taken into consideration in this provision: the coercive fine may not be imposed if there is reason to suspect this party of a criminal offence and the requested material is related to this suspected offence. Although the wording is not strictly limited to natural persons, this exception would seem very unlikely to apply to third parties such as OSPs. Beyond this, the Customs Act does not contain further regulation on coercive fines, which means that the general provisions of the Act on Coercive Fines apply.

Administrative decisions of the Customs, such as decisions on coercive fines, are subject to the administrative review procedure, after which an appeal to the Helsinki Administrative Court is possible. The decision of the Administrative Court may be appealed to the Supreme Administrative Court, if a leave to appeal is granted.⁷⁵ The Customs Act does not specify whether a request for information is an appealable decision as such, nor provide that a decision concerning the obligation must be issued if the obliged party refuses the initial request.⁷⁶ No case law or other information relating to such appeals could be found. As discussed in the following sections, in other sectorial

⁷³ Act on Crime Prevention in the Customs, s 14 sub-ss 1–2.

⁷⁴ See also UCC, Article 15(1), which states that information shall be provided ‘within any time-limit specified’. However, as the general principles of good administration apply also to punitive administrative proceedings and the obligated party must have a practical possibility to adhere to the order, the time-limit cannot be unreasonably short. See Määttä (n. 60), p. 120. Cf. Act on Crime Prevention in the Customs, s 14, according to which subscriber information (and certain other information) can be requested from third parties within a *reasonable* time-limit, and Administrative Procedure Act, s 33(1), according to which time-limits for submitting evidence must be sufficient in view of the nature of the matter.

⁷⁵ See Customs Act, ss 88–90.

⁷⁶ Cf. section 3.1.2 of this report.

frameworks which do not contain a specific provision concerning administrative decisions on obligations to provide information, the prevailing interpretation seems to be that requests for evidence do not constitute administrative decisions.⁷⁷ This would seem likely to be the case in customs enforcement, as well.

3.1.2. Tax enforcement as regards VAT

The two acts concerning the assessment procedure do not mention electronic evidence. Instead, they contain detailed provisions concerning the general and special obligations of third parties to provide information to the Tax Administration. General obligations relate to regular reporting obligations and information transfers that concern the data of many subjects.⁷⁸ In contrast, special obligations are related to situations in which the Tax Administration requests information that is needed for the taxation proceedings concerning a specific taxpayer from a specified third party.⁷⁹

The general provision on the special obligation of any private third party to provide information to the Tax Administration is contained in Section 19 of the Act on the Assessment Procedure. This provision is applicable also in VAT proceedings.⁸⁰ It obligates anyone to provide information relevant to another taxpayer's taxation, or appeals thereof, which is contained in documents in the possession of this third party or that they otherwise have knowledge of, unless they have the right not to testify. The third party may not refuse to give information regarding the financial situation of the taxpayer that is relevant for taxation purposes.

The information must be provided on request. The initial written request, which is delivered to the recipient electronically (often via secure e-mail) or via traditional mail, does not constitute an administrative decision – however, if the request is refused, the law specifically provides that an administrative decision must be issued.⁸¹ The question of which officials

⁷⁷ See sections 3.1.3, 3.1.4 and 3.1.5 of this report.

⁷⁸ Consequently, information reported by third parties due to these general obligations does not, by default, relate to a specific, ongoing investigation. It may serve as a basis for continuous screening and identifying cases for further supervisory measures (together with information filed by taxpayers themselves) and may eventually be used as evidence also in punitive administrative proceedings.

⁷⁹ HE 131/1995 vp, p. 27; T. Räsänen, *Verotusmenettely ja muutoksenhaku*, Helsinki, Alma Talent, 8th ed., 2022, pp. 609, 626–627.

⁸⁰ Act on the Assessment Procedure of Self-assessed Taxes, s 30(1) contains a reference to this provision, as well as to Act on the Assessment Procedure, s 20 (concerning the special obligation of a public authority).

⁸¹ Act on the Assessment Procedure of Self-assessed Taxes, s 52(3). As will be discussed in later sections of this report, the sectorial frameworks in other focus areas do not contain a similar provision.

within the Tax Administration are authorised to make these requests is not regulated on the level of parliamentary acts, but in the internal rules of procedure of the Tax Administration and its units. Typically, such requests may be made by individual tax inspectors or officials assigned to the case.⁸² The law provides that in the request, the taxpayer must be identified by name, bank account number, account transaction, or in another similar way. This entails that requests under Section 19 must concern a specific individual or a limited number of individuals. A set of general conditions or search criteria applying to a large group of people is not appropriate identification in the sense of this provision,⁸³ but requests concerning individuals whom the Tax Administration has not yet been able to identify are possible (e.g., parties of a specific transaction). The Tax Administration may order a third party (unless it is a natural person or a death estate) to provide information through electronic means,⁸⁴ and the information must be provided free of charge.⁸⁵

Beyond this, the procedure and format for transferring information to the Tax Administration are not specified in the law. In relation to requests under Section 19, the Tax Administration has not been delegated the power to issue similar binding orders or instructions regarding the format or other technical details of submissions as in relation to the general obligations.⁸⁶ With regard to certain third parties that information is frequently requested from (e.g., banks), there are established practices regarding how information is transferred, but no universal standards.⁸⁷

Section 19 is a very broad provision: it can apply to various kinds of third parties depending on the nature of the supervision case and what kind of information is required. It does not distinguish between data categories such as content data or traffic data. As tax enforcement is usually focused on the ‘following the money’ approach, it is frequently used to request information regarding bank account transactions and sales and purchases of goods and services. In a VAT enforcement case, it could be used to request transactional data also from online platforms and marketplaces. Although the need for such targeted requests may have been diminished by the recently increased general

⁸² Interview with Sami Peltola, Compliance Manager, Tax Administration (24.6.2024).

⁸³ See Rābinä, (n. 79), pp. 631–632.

⁸⁴ Act on the Assessment Procedure, s 22(5). Section 22 is referenced in Act on the Assessment Procedure of Self-assessed Taxes, s 31(2) and therefore applicable in situations involving VAT enforcement.

⁸⁵ Act on the Assessment Procedure, s 25(1) and Act on the Assessment Procedure of Self-assessed Taxes, s 31(2)).

⁸⁶ Cf., e.g., Act on the Assessment Procedure of Self-assessed Taxes, s 29(8) and Act on the Assessment Procedure, s 15(9).

⁸⁷ Interview with Sami Peltola, Compliance Manager, Tax Administration (24.6.2024).

reporting obligations,⁸⁸ Section 19 can still be used in an individual case to complement the regular data flows, as needed.⁸⁹ Potentially, Section 19 could also be interpreted to enable requesting subscriber information from telecommunications operators and other OSPs, but there does not appear to be any established practice or case law on the issue.⁹⁰ However, the aforementioned limits in the national constitutional doctrine would seem to preclude its use as a substitute for telecommunications interception or traffic data monitoring.

The Tax Administration may perform tax audits in relation to VAT enforcement.⁹¹ Tax audits are connected to third party obligations to provide information in two ways. Firstly, specific information required for a tax audit may be acquired from third parties under Section 19. Secondly, tax audits may also be conducted with the specific objective to gather comparison data from another taxpayer (comparison data audit).⁹² Comparison data audits can be understood as a type of special obligation to provide information,⁹³ and they are often conducted in the form of a request for a large dataset corresponding to search criteria specified in the request. This request can be made without identifying the taxpayers concerned. Comparison data audits are typically used for risk management purposes and for identifying cases for further

⁸⁸ In particular, the so-called DAC7 Directive (Council Directive (EU) 2021/514 of 22 March 2021 amending Directive 2011/16/EU on administrative cooperation in the field of taxation) subjects digital platform operators to new reporting requirements concerning information relating to transactions and sellers operating on their platform. Service providers that must report this information in Finland may submit it electronically in XML format through a portal operated by the Tax Administration (Ilmoitin.fi), which is used also for submitting other data to the Tax Administration. See Act on the Assessment Procedure, s 17f and Act Governing the Information-reporting Requirement of Platform Economy Operators to Provide Information in the Field of Taxation (*laki digitaalisen alustatalouden toimijoiden tiedonantovelvollisuudesta verotuksen alalla*, 1267/2022). See also Tax Administration, ‘The information-reporting requirement of a Reporting Platform Operator (DAC7)’ 2023, online <https://www.vero.fi/en/detailed-guidance/guidance/209369/the-information-reporting-requirement-of-a-reporting-platform-operator--dac7/>.

⁸⁹ Interview with Sami Peltola, Compliance Manager, Tax Administration (24.6.2024).

⁹⁰ While a representative of the Tax Administration considered this a possible interpretation, he was unable to confirm whether such requests have been made in practice (interview with Sami Peltola, Compliance Manager, Tax Administration (24.6.2024)).

⁹¹ Section 24 of the Act on the Assessment Procedure of Self-assessed Taxes. On tax audits relating to other taxes, see Act on the Assessment Procedure, s 14.

⁹² Act on the Assessment Procedure, s 21 and Act on the Assessment Procedure of Self-assessed Taxes, s 31(2)).

⁹³ Räsänen, (n. 79), p. 627.

supervisory measures, and therefore do not necessarily relate to a specific ongoing investigation.⁹⁴

When conducting a tax audit, access to bookkeeping data and other relevant materials is primarily gained through the cooperation of the targeted taxpayer, who is legally obligated to provide full access to any relevant materials stored electronically even if these are stored in external services or abroad.⁹⁵ If the relevant material is in electronic format, audits may be performed as e-audits without any physical visits to the premises of the taxpayer or their accounting company.⁹⁶ In practice, the Tax Administration may be provided with, e.g., direct access to the information system of the accounting company. However, bookkeeping data or other such material (or access to systems) is typically not requested directly from service providers.⁹⁷

A request for specific information or comparison data may be followed by discussions and negotiations between the third party and the Tax Administration, and these consultations often result in the third party submitting the required information.⁹⁸ However, as already mentioned, in the event that the third party refuses to provide the requested information, an administrative decision must be made.⁹⁹ It is further specifically provided that the party obligated to provide information may appeal this decision.¹⁰⁰ While requests for information were rarely questioned or refused in the past, the issuing of administrative decisions, as well as appeals against them, have become more common in the last few years.¹⁰¹

The acts concerning the assessment procedure do not contain provisions on coercive fines as an enforcement measure in regard to the obligations to provide information. However, a negligence penalty may be imposed by the Tax Administration also to third parties who fail to provide requested information.¹⁰² In most situations, a negligence penalty cannot be imposed on

⁹⁴ Interview with Sami Peltola, Compliance Manager, Tax Administration (24.6.2024); Tax Administration, 'Good tax auditing practice' 2017 (last updated 2021), online https://www.vero.fi/en/detailed-guidance/guidance/49204/good_tax_auditing_practic/, 3.2 and 8. Note that this is an unofficial English translation, and that the current official version of this instruction is from 2018.

⁹⁵ See Act on the Assessment Procedure of Self-assessed Taxes, s 24 sub-ss 1–2. See also Decree on the Assessment Procedure (*asetus verotusmenettelystä*, 763/1998), ss 2–4.

⁹⁶ See Tax Administration, 'Good tax auditing practice' 2017 (last updated 2021), online https://www.vero.fi/en/detailed-guidance/guidance/49204/good_tax_auditing_practic/, 5.2.

⁹⁷ Interview with Sami Peltola, Compliance Manager, Tax Administration (24.6.2024).

⁹⁸ Interview with Sami Peltola, Compliance Manager, Tax Administration (24.6.2024).

⁹⁹ Act on the Assessment Procedure of Self-assessed Taxes, s 52(3).

¹⁰⁰ Act on the Assessment Procedure of Self-assessed Taxes, s 62(2).

¹⁰¹ Interview with Sami Peltola, Compliance Manager, Tax Administration (24.6.2024).

¹⁰² Act on the Assessment Procedure, s 22a. Depending on the circumstances, the maximum amount is 2.000 €, 5.000 €, or 15.000 €. See also the references to this provision in Act on

a natural person or a death estate,¹⁰³ but this does not limit its potential use against an OSP. A third party that is imposed a sanction for failure to provide information may appeal this decision.¹⁰⁴ In practice, negligence penalties have very rarely been imposed for failure to provide information.¹⁰⁵

As regards administrative decisions relating to VAT proceedings, including decisions concerning provision of information and sanctions, the Act on the Assessment Procedure of Self-assessed Taxes contains special rules on review and appeals. Requests for review are sent to the Adjustment Board, and the decisions of this Board may be further appealed to the Administrative Court and, with leave to appeal, to the Supreme Administrative Court. In certain situations, a direct appeal to the Supreme Administrative Court is possible after the decision of the Adjustment Board.¹⁰⁶

3.1.3. Punitive enforcement in the area of banking law and financial markets

Chapter 3 of the FSA Act contains detailed regulation on the FIN-FSA's rights to receive information from various parties. These provisions mainly concern supervised entities and other financial market participants,¹⁰⁷ undertakings connected to them,¹⁰⁸ auditors¹⁰⁹ and other authorities¹¹⁰. However, Section 19(3) of the FSA Act applies to any third party that is not covered by the other obligations set in Section 19. It provides that the FIN-FSA has 'the right to obtain, for carrying out a specific supervisory measure,

the Assessment Procedure of Self-assessed Taxes, ss 31(2) and 29(7). Negligence penalties concerning certain obligations defined in the Value Added Taxes Act (*arvonlisäverolaki*, 1501/1993, VAT Act) and other acts governing various self-assessed taxes are regulated in Act on the Assessment Procedure of Self-assessed Taxes, s 39. In some situations, neglecting an obligation to provide information may also lead to criminal punishment. See Act on the Assessment Procedure, s 87 (which is *not* referenced in the Act on the Assessment Procedure for Self-assessed Taxes).

¹⁰³ See Act on the Assessment Procedure, s 22a(6).

¹⁰⁴ Act on the Assessment Procedure of Self-Assessed Taxes, s 62(2).

¹⁰⁵ Interview with Sami Peltola, Compliance Manager, Tax Administration (24.6.2024).

¹⁰⁶ See Act on the Assessment Procedure of Self-assessed Taxes, c 10 (in particular ss 58–64 and 67–68).

¹⁰⁷ FSA Act, ss 18 and 21. Under s 18(4), parties that, e.g., manage information systems for supervised entities are obligated to provide information in the same way as supervised entities themselves.

¹⁰⁸ FSA Act, s 23.

¹⁰⁹ FSA Act, s 19 sub-ss 1 and 4. As per sub-s 2, the provisions on auditors laid down in sub-s 1 shall also apply to any other person who has a legal obligation to have, or has consented to having, an opinion or other document drawn up by them attached to a prospectus as referred to in Securities Markets Act, c 3 s 1.

¹¹⁰ FSA Act, ss 20, 20a and 20b.

any information that is necessary for the exercise of supervision from persons other than those referred [in Subsections 1 and 2] who, with justifiable cause, may be presumed to have information necessary for carrying out such supervisory measures'. Section 21(2)(3) contains a similar provision in relation to the special right to information related to marked abuse and supervision of the Benchmark Regulation. Additionally, Section 21(2)(1) covers those who act for, or on behalf of, a supervised entity or other financial market participant, which could be interpreted to include various kinds of service providers.

Notably, Section 24 of the FSA Act, concerning inspections, mentions certain categories of electronic evidence.¹¹¹ Among other things, the FIN-FSA specifically has the right to receive recordings of telephone conversations and records of electronic communications, other telecommunications data and information systems for inspection.¹¹² In addition to supervised entities, parties that for example manage information systems for supervised entities are obligated to provide documents and records for inspection.¹¹³ Likewise, persons and entities obligated by Sections 19 and 21 must provide documents and records containing information covered by these provisions for inspection.¹¹⁴

Even though the aforementioned provisions are worded broadly, in practice they do not cover all data held by third parties, and in some respects, the FIN-FSA does not have as extensive investigative powers as some of its European counterparts. In particular, the national legislation does not empower the FIN-FSA to obtain traffic data directly from telecommunications operators, even though MAR, Article 23(2)(h) requires the supervisory authorities to have this power 'insofar as permitted by national law'. As already mentioned, under Finnish law, traffic data monitoring can only be carried out by criminal justice and intelligence authorities, and empowering the FIN-FSA to do this would be constitutionally problematic.¹¹⁵ Therefore, traffic data (and content data) related to electronic communications can only be acquired from supervised entities under Section 24 of the FSA Act. Further, the interpretation of the FIN-FSA has been that the provisions on its rights to receive information do not enable it to request

¹¹¹ The FIN-FSA's powers of inspection are also regulated in AML Act, c 7 s 3 and CPCPA Act, s 8. While these provisions do not mention specific data categories or cooperation by third parties, the AML Act provision does mention information systems and also specifically enables conducting of inspections via remote connection.

¹¹² FSA Act, s 24(1).

¹¹³ FSA Act, s 24(2); see also s 18(4) on the obligation of these parties to otherwise provide documents.

¹¹⁴ FSA Act, s 24(3).

¹¹⁵ See HE 66/2008 vp, pp. 53–54 and HE 65/2016 vp, p. 27.

subscriber information from OSPs for the purposes of identifying, e.g., authors of blog posts or social media publications.¹¹⁶

The FSA Act does not contain any specific rules on the procedure or technical format of data transfers relating to the provisions that enable it to receive information from third parties.¹¹⁷ If the FIN-FSA needs information from third parties, this is usually done via a written request specifying the information in question and the legal basis for the request. Such a request is usually signed by the Head of Division and the official assigned to the investigation, or in some cases by the latter alone (as per internal rules of procedure). The FIN-FSA does not consider this request to constitute an appealable administrative decision, and ignoring it does not carry direct consequences.¹¹⁸

As per Section 33a, the FIN-FSA may impose coercive fines. Obligations to provide information and cooperate with inspections, including those applying to third parties, can be enforced with a coercive fine ‘provided that the negligence is not negligible’,¹¹⁹ which implies that a coercive fine cannot be attached to the first request addressed to a third party. It is also specified that a coercive fine may not be imposed on a natural person to enforce compliance with an obligation to provide information if there is reason to suspect this person of a criminal offence and the information is related to this matter.¹²⁰ This provision is similar to the aforementioned self-incrimination exception in the Customs Act. However, the FSA Act provision is unambiguously limited to natural persons. Therefore, it does not prevent the imposition of coercive fines against OSPs that are legal persons (even in the event that the requested information relates to something for which the OSP in question could face corporate criminal liability).

As usual, decisions on coercive fines are appealable administrative decisions. Since 2018, all decisions of the FIN-FSA can be appealed to the Helsinki Administrative Court, and further to the Supreme Administrative

¹¹⁶ Interview with Pia Ovaska, Chief Legal Advisor, Financial Supervisory Authority (13.6.2024). Content published anonymously or pseudonymously in investment blogs or on social media may be relevant for market manipulation investigations and the supervision of investment recommendations.

¹¹⁷ However, under FSA Act, s 18, the FIN-FSA may issue regulations (applicable to supervised entities) regarding the regular provision of information for supervisory purposes, including the manner in which this information is provided. The power to issue similar regulations has been delegated to the FIN-FSA also in Securities Markets Act, AML Act and other parliamentary acts. Some regulation on technical details of certain notifications and submissions to supervisory authorities is also found in, e.g., EU-level implementing acts, such as Commission Implementing Regulations (EU) 2016/378 and (EU) 2022/1210.

¹¹⁸ Interview with Pia Ovaska, Chief Legal Advisor, Financial Supervisory Authority (13.6.2024).

¹¹⁹ FSA Act, s 33a(2).

¹²⁰ FSA Act, s 33a(3).

Court with a leave to appeal, under the Administrative Judicial Procedure Act.¹²¹ Prior to this, appeals on decisions concerning administrative sanctions under the FSA Act were directed to the Market Court.¹²²

In 2013–2023, the FIN-FSA imposed a total of 20 public warnings and 59 monetary sanctions.¹²³ Based on a review of the public versions of decisions published on the FIN-FSA website (including four decisions from 2024),¹²⁴ it seems that the FIN-FSA typically does not request specific evidence from third parties.¹²⁵ Its decisions on sanctions are mainly based on its own observations and information provided by supervised entities – typically the ones that are subsequently imposed sanctions – and other entities with reporting obligations.¹²⁶ None of the decisions specifically referred to

¹²¹ See FSA Act, s 73.

¹²² Further, before this amendment (1071/2017, which entered into force on 3.1.2018), the FIN-FSA could independently impose penalty payments up to 1.000.000 €, but penalty payments higher than this were laid down by the Market Court. Decisions of the Market Court could be appealed to the Supreme Administrative Court.

¹²³ Financial Supervisory Authority, ‘Sanctions, requests for investigation and cases of securities market inspections’ 2024 (last updated), online <https://www.finanssivalvonta.fi/en/statistics/Sanctions-requests-for-investigation-and-cases-of-securities-market-inspections/>. The monetary sanctions include 36 administrative fines and 23 penalty payments. Additionally, the FIN-FSA made a total of 54 requests for police investigation during this period. In the same period, the FIN-FSA handled a total of 1.355 supervision cases related to trading in securities market and the disclosure obligations. Out of these cases, approximately 59 percent related to abuse of insider information, 26 percent to market manipulation and 12 percent to disclosure obligations.

¹²⁴ The decisions (in Finnish or Swedish) and English summaries are available at the FIN-FSA website. Financial Supervisory Authority, ‘Supervisory measures’ 2024 (last updated), online <https://www.finanssivalvonta.fi/en/about-the-fin-fsa/powers-and-funding/powers-and-authority/supervisory-measures/>. These decisions include administrative sanctions based on both FSA Act and AML Act.

¹²⁵ However, in at least one case, information had been requested and received from a securities broker used by the supervised entity under investigation (Decision of 26.5.2015, FIVA 37/02.04/2014 (Finnvera Oyj)). This decision also references information received from the national central securities depository, Euroclear Finland Oy. As the FIN-FSA has direct access to the book-entry system operated by Euroclear Finland Oy for supervisory purposes, specific requests are not needed for this information (interview with Pia Ovaska, Chief Legal Advisor, Financial Supervisory Authority (13.6.2024)). As a supervised entity, Euroclear Finland Oy is generally obligated to provide information to the FIN-FSA under FIN-FSA Act, s 18.

¹²⁶ This was also affirmed in the interview with Pia Ovaska, Chief Legal Advisor, Financial Supervisory Authority (13.6.2024). – The FIN-FSA may also employ outside expert advisers, such as auditors, to clarify matters requiring special expertise under FSA Act, s 34. While these experts may have access to information provided by third parties under, e.g., s 19, they typically evaluate documents provided by the supervised entity, as for example in the case concerning Navi Group Oy (Decision of 5.11.2014, FIVA 5/02.04/2014 (Navi Group Oy) and the subsequent Market Court Decision of 23.9.2015, MAO:636/15, and Supreme Administrative Court Decision ECLI:FI:KHO:2016:T5295).

requests based on FSA Act, Section 19(3) or 21(2), or any evidence received from OSPs. It is noteworthy that a large share of these cases concerned delayed or neglected reporting or notifications.¹²⁷ Typically, establishing these kinds of violations is rather straightforward and does not require complex evidence. In cases involving other kinds of violations, the imposition of an administrative sanction often followed inspections that had been carried out by the FIN-FSA. While the published decisions do not describe the role of third parties in executing these inspections, the FIN-FSA primarily gains access to various information systems through the cooperation of supervised entities and therefore does not generally approach, e.g., cloud service providers directly.¹²⁸

3.1.4. Competition law enforcement

Section 33 of the Competition Act concerns the obligations of various entities and persons to provide information to the FCCA. Private and public entities and – since the implementation of the ECN+ Directive¹²⁹ – natural persons are obligated to provide all information and documents that are needed to investigate the contents, purpose and impact of a restriction of competition at the request of the FCCA. Undertakings and other entities are also obligated to clarify the competitive conditions, and their obligations further extend to matters concerning control of concentrations and competition neutrality.¹³⁰

Section 33 is worded very broadly. It generally covers all kinds of third parties in addition to the supervised undertakings, and it would seem to cover all data categories without distinction. There are some specified limitations to these obligations that concern natural persons¹³¹ and undertakings under

¹²⁷ The FIN-FSA may impose administrative fines under FSA Act, s 38 (and in some situations, other administrative sanctions) for various obligations applying to banking and financial market actors that concern publishing information or notifying the FIN-FSA and/or other parties of certain events.

¹²⁸ Interview with Pia Ovaska, Chief Legal Advisor, Financial Supervisory Authority (13.6.2024).

¹²⁹ Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market.

¹³⁰ As Competition Act, s 33(1) applies to public entities, there is some overlap between s 39(2) (concerning the FCCA's right to receive information from other authorities) and s 33(1).

¹³¹ Natural persons are not obligated to provide information concerning special categories of personal data or data relating to criminal convictions and offences, or documents falling under the legal professional privilege (Competition Act, s 33(2). This exception was added by the parliamentary Commerce Committee after the Constitutional Law Committee had required more precision. As competition law concerns the business activities of undertakings, the information needs of the supervisory authorities were not seen to be focused on sensitive

investigation,¹³² but these do not apply to third parties that are legal persons, such as OSPs. Nevertheless, in line with the aforementioned constitutional limitations and interpretations concerning corresponding general provisions in other sectors, the FCCA does not interpret Section 33 to enable requesting communications data held by, e.g., telecommunications operators directly from these intermediaries (i.e., as a substitute for telecommunications interception or traffic data monitoring, which are only available to the criminal justice authorities). Section 33 could potentially be interpreted to allow the FCCA to request subscriber information in order to identify users of communications services or recipients or senders of electronic messages. However, there is no established practice or frequent need for this, as the individuals who have participated in electronic communications that are relevant for the investigation can often be identified with the cooperation of the involved entities.¹³³

The obligation to provide information under Section 33 is created after a specific request.¹³⁴ Requests may be made more or less formally (e.g., via e-mail), and according to the FCCA, they do not, as such, constitute appealable administrative decisions.¹³⁵ The Market Court has recently accepted the FCCA's position that requests for information are not eligible to be appealed against unless they are enforced with a coercive fine.¹³⁶ However, it should be noted that this case concerned requests addressed to the suspected

personal data but on information related to economic activity. See TaVM 14/2021 vp, p. 11 and PeVL 8/2021 vp, pp. 6–8.

¹³² As part of their defence rights in competition law investigations, undertakings have no obligation to provide documents containing confidential correspondence between an outside legal consultant and a client (Competition Act, s 38(3)). The defence rights of undertakings further include, e.g., the right to receive information regarding their status in the investigations and what acts they are suspected of. Further, undertakings are not obligated to admit to violating the norms regarding restrictions of competition or market abuse in their responses to the authorities.

¹³³ Interview with Vilhelmiina Ihamäki, Senior Adviser and Kalle Markkanen, Senior Specialist, Finnish Competition and Consumer Authority (25.6.2024). However, within inspections (further discussed later in this section), competition authorities are empowered to access electronic messages which are accessible to the suspected entity 'irrespective of whether they appear to be unread or have been deleted'. See ECN+ Directive, Recital 32. See also Recital 73, which concerns the admissibility of electronic communications as evidence before national competition authorities, regulated in Article 32.

¹³⁴ HE 210/2020 vp, p. 99.

¹³⁵ Interview with Vilhelmiina Ihamäki, Senior Adviser and Kalle Markkanen, Senior Specialist, Finnish Competition and Consumer Authority (25.6.2024).

¹³⁶ Decision of 24.6.2024, MAO:375/2024. The decision has been appealed to the Supreme Administrative Court, and therefore it is not final.

entity, not a third party.¹³⁷ Despite the wording, Section 33 has been interpreted to provide the legal basis also for a service produced by a private company that allows the FCCA direct access to data concerning public tenders. These data are typically analysed for screening and identifying cases for further supervisory measures.¹³⁸

The Competition Act does not regulate the technical details of how evidence is to be transferred to the FCCA. However, according to Section 33(5), the information shall, whenever requested, be submitted in writing, and the information may also be submitted using a technical interface or other electronic means.¹³⁹ When requests concern large datasets, practical issues relating to, e.g., technical aspects of data transfers, data security and pseudonymisation are often preliminarily discussed between the FCCA and the party providing the information already before the request is officially sent.¹⁴⁰

The Competition Act also grants the FCCA the competence to carry out on-site inspections both in the business premises of an undertaking (Section 35) and in other premises (Section 36).¹⁴¹ It is noteworthy that in connection with on-site inspections, information may also be requested from service providers. In Section 37(1), it is specified that the FCCA has the right to examine the business correspondence, accounts, data processing records as

¹³⁷ Administrative Judicial Procedure Act, s 6(2) declares decisions relating solely to the preparation of a matter ineligible for review by appeal. This covers actions such as requests for statements and possibly other actions taken to clarify facts in an investigation. However, issues relating to the preparation of a matter are not fully outside judicial review, because they can be raised in the appeal concerning the final decision, i.e., the decision concerning a penalty payment or other sanction (see O. Mäenpää, *Oikeudenkäynti hallintoasioissa*, Helsinki, Alma Talent, 2019, p. 84). As third parties may not appeal the final decision in punitive administrative proceedings, it could be argued that requests for information addressed to third parties should be appealable.

¹³⁸ Interview with Vilhelmiina Ihamäki, Senior Adviser and Kalle Markkanen, Senior Specialist, Finnish Competition and Consumer Authority (25.6.2024). The service is provided by Cloudia Oy. See also Finnish Competition and Consumer Authority, 'Tilastollisten menetelmien hyödyntäminen kartellien paljastamisessa' Kilpailu- ja kuluttajaviraston Policy Brief 1/2023, online <https://www.kkv.fi/uploads/sites/2/2023-01-policybrief-tilastollisten-menetelmien-hyodyntaminen.pdf>. The interviewees also highlighted the use of open source intelligence (OSINT) methods and publicly available information in competition law enforcement.

¹³⁹ In a similar fashion, Competition Act, s 39(4) provides that exchange of information between authorities may be carried out using a technical interface or by other electronic means.

¹⁴⁰ Interview with Vilhelmiina Ihamäki, Senior Adviser and Kalle Markkanen, Senior Specialist, Finnish Competition and Consumer Authority (25.6.2024).

¹⁴¹ Inspections can only be carried out in the premises of third parties in case there is a reasonable suspicion that business books and records relating to the subject matter of the inspection are being kept there, and only with prior authorisation from the Market Court. See Competition Act, s 36 sub-ss 1 and 5.

well as any other records and data of the undertaking which may be relevant for supervisory purposes. According to Subsection 2, the FCCA further has the right to receive all the information necessary for the inspection also from service providers (i.e., companies that handle communications or information at the request of an undertaking subject to the inspection or otherwise as part of a service provided to it). If costs are incurred by the service provider cooperating with the inspection, the undertaking subject to the inspection is responsible for these costs, unless otherwise agreed.

The Competition Act empowers the FCCA to impose coercive fines to ensure compliance with its various decisions. In case of non-compliance, the payment can be ordered by the Market Court.¹⁴² A coercive fine may not be imposed on a natural person in order to enforce an obligation to provide information under Section 33, or to ensure compliance with the summons for an interview under Section 34.¹⁴³ This exception is clearly limited to natural persons, and therefore does not prevent the imposition of coercive fines to OSPs that are obligated to provide information. However, coercive fines may be imposed on undertakings (and associations of undertakings) to ensure that their representatives comply with the summons for an interview. Although this is not specifically stated in the law, this possibility has been interpreted to apply only to the entity that is under investigation, not to a third party such as the current employer of a former employee of the suspected undertaking.¹⁴⁴ In line with this interpretation, if an employee of an OSP was summoned for an interview, a coercive fine could not be imposed on the OSP to enforce compliance with the summons.

Further, as already mentioned, Competition Act, Section 37a (which was added to the law in 2021) allows the FCCA to make a proposal to the Market Court on a penalty payment for intentional or negligent non-compliance with various procedural obligations relating to investigations concerning restrictions of competition. The possible grounds for a penalty payment include giving false, insufficient or misleading information or failing to provide information by a given time-limit in response to a request under Section 33 and obstructing an inspection under Section 35. This kind of penalty payment may be targeted at an undertaking or an association of undertakings. While in most scenarios this would mean the undertaking that is suspected of violating the rules concerning restrictions of competition, the wording of the provision does not specifically exclude entities that are no longer or were never suspected of competition law violations, nor

¹⁴² Competition Act, s 46(1).

¹⁴³ Competition Act, s 46(4).

¹⁴⁴ Interview with Vilhelmiina Ihämäki, Senior Adviser and Kalle Markkanen, Senior Specialist, Finnish Competition and Consumer Authority (25.6.2024).

undertakings providing services to the suspected undertaking.¹⁴⁵ Despite the ambiguous wording, this provision is unlikely to apply to third parties such as OSPs. In relation to third parties, a coercive fine would arguably be a more suitable enforcement measure than a penalty payment, which has a more punitive character and is intended as a punishment for relatively severe violations of procedural obligations.¹⁴⁶

As of yet, there is very limited administrative practice or case law regarding coercive fines and Section 37a penalty payments, and undertakings usually comply with requests for information by the FCCA.¹⁴⁷ As the Market Court is responsible for imposing punitive administrative sanctions and ordering the payment of coercive fines under the Competition Act, in these situations an appeal to the Supreme Administrative Court is possible without a leave to appeal. Decisions of the FCCA, such as imposing coercive fines as an enforcement measure, can be appealed to the Market Court as the first instance.¹⁴⁸

A review of recent penalty payment proposals by the FCCA¹⁴⁹ revealed no mentions of requests for evidence directed at third parties such as OSPs. Based on these cases, on-site inspections – mostly carried out under Competition Act, Section 35, and sometimes additionally under Section 36 – seem to play the main role in the evidence-gathering activities of the FCCA in punitive administrative investigations.¹⁵⁰ Additional written statements and oral evidence are typically requested from involved parties and their former and current representatives and employees under Sections 33 and 34. If

¹⁴⁵ Obstruction of an inspection under Competition Act, s 36 is not included in the list of sanctionable violations in s 37a(1), which could be interpreted to suggest that penalty payments are at least not primarily intended to be targeted at third parties.

¹⁴⁶ As coercive fines and penalty payments have somewhat different functions, it may be possible to impose both a coercive fine and a penalty payment in the same case (e.g., when it is later revealed that information provided under the threat of a coercive fine is false). See HE 210/2020 vp, pp. 104–105, 117.

¹⁴⁷ Interview with Vilhelmiina Ihamäki, Senior Adviser and Kalle Markkanen, Senior Specialist, Finnish Competition and Consumer Authority (25.6.2024).

¹⁴⁸ See Competition Act, ss 49a and 49b; HE 210/2020 vp, p. 125; Market Court Decision of 24.6.2024, MAO:375/2024.

¹⁴⁹ The review targeted the public versions of 11 proposals (from 2012 to 2024) published on the FCCA website. Finnish Competition and Consumer Authority, ‘Esitykset markkinaoikeudelle’ 2024 (last updated), online <https://www.kkv.fi/paatokset/kilpailuasiat/esitykset-markkinaoikeudelle/>.

¹⁵⁰ The importance of inspections in producing evidence for punitive administrative proceedings was affirmed in the interview with Vilhelmiina Ihamäki, Senior Adviser and Kalle Markkanen, Senior Specialist, Finnish Competition and Consumer Authority (25.6.2024)). See also R. Autio, ‘Menettely kilpailuviranomaisen yllätystarkastuksilla aineiston siirryttyä paperilta pilvipalvelimille’ *Liikejuridiikka – Finnish Business Law Journal*, 2023, vol. 9, no. 3, pp. 24–25 (on the significance of inspections and ‘dawn raids’ in cartel investigations).

information is requested from a party that is not under investigation, this third party is often a company or a person that operates in the same market and may, e.g., possess information on the market conditions.

Although electronic evidence does not seem to be often requested from third parties, its importance in competition investigations has been noted in recent literature.¹⁵¹ While electronic evidence is mainly acquired from the suspected entities, it should be noted that the aforementioned review of penalty payment proposals does not reveal what roles third parties may have played during inspections.¹⁵² According to information received in an interview,¹⁵³ however, inspections are carried out primarily with the cooperation of the suspected entities, who are legally obligated to cooperate and may be imposed Section 37a penalties for failure to provide access to, e.g., information stored on the server of an external service provider.¹⁵⁴ Nevertheless, as a last resort, access to relevant data or other assistance in carrying out the inspection could be requested directly from such a service provider, as permitted by Competition Act, Section 37(2).¹⁵⁵

3.1.5. GDPR enforcement

In relation to GDPR enforcement, the powers of the supervisory authorities are regulated at the EU level in GDPR, Article 58. At the national level, complementary rules on the right of the Data Protection Ombudsman to obtain information and carry out inspections – as permitted by GDPR, Article 58(6) – are provided in Section 18 of the Data Protection Act.

¹⁵¹ *Ibid.*, pp. 30–31. Autio notes indications of the development of the FCCA's forensic capabilities and points out that in its recent sanction proposals, the FCCA has relied on, e.g., metadata from Excel files, messages deleted by user, and WhatsApp messages.

¹⁵² A recent penalty payment proposal (of 22.5.2024, KKV/376/14.00.00/2023 (Attendo Suomi Oy)) concerns the deletion of WhatsApp messages from a manager's work phone during an on-site inspection. According to the public version of the proposal, the phone was analysed with the Cellebrite Physical Analyzer software and several deleted messages were later recovered from iCloud backups. Access to these backups was gained with the cooperation of the company (and not with a request addressed to Apple), as confirmed in the interview with Vilhelmiina Ihamäki, Senior Adviser and Kalle Markkanen, Senior Specialist, Finnish Competition and Consumer Authority (25.6.2024).

¹⁵³ Interview with Vilhelmiina Ihamäki, Senior Adviser and Kalle Markkanen, Senior Specialist, Finnish Competition and Consumer Authority (25.6.2024).

¹⁵⁴ The 'access principle' in competition law inspections has a basis in EU law, namely the ECN+ Directive, Article 6(1)(b), which provides that competition authorities shall be empowered to have the right to access any information which is accessible to the entity subject to the inspection. See Autio, (n. 150), p. 13.

¹⁵⁵ According to the interpretation of the FCCA, such requests during inspections would not be based on Competition Act, s 33, but the provisions concerning inspections (interview with Vilhelmiina Ihamäki, Senior Adviser and Kalle Markkanen, Senior Specialist, Finnish Competition and Consumer Authority (25.6.2024)).

Subsection 1 states that in addition to what is provided in GDPR, Article 58(1), ‘the Data Protection Ombudsman has the right, notwithstanding non-disclosure provisions, to obtain, free of charge, access to information that is necessary for the performance of their tasks’.¹⁵⁶ Under this provision, the right to obtain information is not limited to controllers and processors.¹⁵⁷ This means that information can be requested from any public and private third parties (within Finnish jurisdiction) that possess relevant evidence, regardless of whether they process personal data on behalf of the controller that is under investigation or not. However, as most (if not all) OSPs are controllers and/or processors, the significance of this difference in the European and Finnish provisions is arguably limited in relation to requests for evidence addressed to OSPs.

Section 18 does not differentiate between any data categories and could therefore be construed to cover all possible data held by OSPs, as long as these data are needed in the administrative investigation. However, the constitutional limitations which have been discussed earlier apply to GDPR enforcement in a similar fashion. Like the general provisions in other sectors, Section 18 should not be interpreted as enabling requests targeting communications data held by telecommunications operators directly from these intermediaries, or to be used otherwise as a substitute for covert telecommunications interception or traffic data monitoring.

Section 18 is formulated as a right of the Data Protection Ombudsman, and it does not contain specific procedural rules on how this right is implemented. In the absence of more specific rules, the *lex generalis* norms of the Administrative Procedure Act are applicable, and requests for evidence can be sent in accordance with the general provisions concerning requests for statements or evidence.¹⁵⁸ Generally, the initial request is made in written form as a letter that specifies the case the request relates to, the legal bases for the request, the requested information, and options on how this information can be submitted (e.g., secure e-mail or traditional mail).¹⁵⁹ The

¹⁵⁶ Additionally, Data Protection Act, s 18(2) contains conditions on inspections carried out in premises used for permanent residence. These are allowed only if this is necessary for examining the circumstances being inspected and if a well-founded and specific reason exists in the case for suspecting that provisions on the processing of personal data have been or are being infringed in a manner that may be sanctioned with an administrative fine or a criminal punishment.

¹⁵⁷ Cf. GDPR, Article 58(1). According to the government proposal (HE 9/2018 vp, p. 100), Data Protection Act, s 18 is specifically meant to expand the Data Protection Ombudsman’s right to receive information beyond what is provided in the GDPR, but the law drafting materials do not discuss in detail which kind of information might be needed that is not covered by the GDPR powers.

¹⁵⁸ Administrative Procedure Act, ss 31–33.

¹⁵⁹ Oral requests for documents or other questions can be made in connection with on-site inspections, but they must also be documented.

request for information is not considered an appealable administrative decision, and it can usually be made independently by the official assigned to prepare the case.¹⁶⁰

Unlike GDPR, Article 58(1)(a), Section 18 does not specifically mention the power to issue an order. Nevertheless, the wording of Section 22 implies that an order to provide information may be issued also when relying on the domestic provision, as it states that to enforce compliance with an order to provide information under Section 18(1), a coercive fine may be imposed.¹⁶¹ However, as the law does not specify whether such an order constitutes an appealable administrative decision in itself, it is somewhat unclear whether such an ‘order’ can be differentiated from a simple ‘request’ for information.

As per GDPR, Article 58(4), the exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process. This would seem to suggest that orders to provide information, even when based on the additional national powers allowed by GDPR, Article 58(6), should be eligible for some judicial remedy. It could be argued that the right to appeal might therefore be necessary when the order is addressed to a party other than the one under investigation (which may appeal against the final decision). On the other hand, it could be argued that the third party may simply refuse to fulfil an order if it is not backed with a coercive fine and cannot be legally enforced otherwise,¹⁶² and therefore there would be no need for any additional remedy. There does not appear to be any established practice or case law relating to appealable orders to provide information issued without issuing a coercive fine.¹⁶³

¹⁶⁰ Interview with Heikki Huhtiniemi, Senior Inspector, Office of the Data Protection Ombudsman (26.6.2024); Rules of Procedure of the Office of the Data Protection Ombudsman, s 26 (*Tietosuojavaltuutetun toimiston työjärjestys*, 24.4.2023, 6897/01/23, online https://www.finlex.fi/data/tsv/TSV_tyojarjestys_FI.pdf). The officials assigned to prepare the case are usually Senior Inspectors, and depending on the situation they may consult the Data Protection Ombudsman or the Deputy Data Protection Ombudsmen before making the request.

¹⁶¹ In Data Protection Act, s 22, the power to impose coercive fines is granted to the Data Protection Ombudsman. The Ombudsman also has the power to set the rules of procedure of their office under Data Protection Act, Section 9(3). Rules of Procedure of the Office of the Data Protection Ombudsman, s 14(2) designates matters concerning coercive fines (as well as some measures under GDPR, Article 58(2)) to the Sanctions Board in order to secure uniformity.

¹⁶² However, the possibility of relying on executive assistance by the Police in these situations has been subject to some speculation (see also section 5 of this report). If such an enforcement method was indeed available, this would further increase the need for an effective remedy.

¹⁶³ Interview with Heikki Huhtiniemi, Senior Inspector, Office of the Data Protection Ombudsman (26.6.2024).

As regards coercive fines, the privilege against self-incrimination and potential overlaps between administrative and criminal sanctions¹⁶⁴ have been addressed with an exception similar to the ones in the FSA Act and the Competition Act: a coercive fine may not be imposed on a natural person if there is reason to suspect this person of a criminal offence and the requested information relates to this suspected offence.¹⁶⁵ Again, this limitation bears no relevance for OSPs that are legal persons, which can – in theory – always be imposed coercive fines if they refuse or fail to provide information. However, in practice, coercive fines are imposed very rarely, if ever, to enforce orders to provide information.¹⁶⁶ If a coercive fine is imposed, this is always a decision that can be appealed. Decisions of the Data Protection Ombudsman and the Sanctions Board may be appealed to the Administrative Court, and further to the Supreme Administrative Court if it grants a leave to appeal, under the general rules of the Administrative Judicial Procedure Act.¹⁶⁷

While Section 18 gives the Data Protection Ombudsman a broad right to any necessary information from third parties, in practice it is rarely used as a basis for requesting evidence from OSPs or other private third parties.¹⁶⁸ Based on a review of 23 decisions of the Sanctions Board from 2020–2024¹⁶⁹ and information received in an interview,¹⁷⁰ the information required for

¹⁶⁴ While this potential exists, it has somewhat decreased due to the fact that in Finland, administrative sanctions under the GDPR have in large part replaced criminal punishment in relation to violations and non-compliance with data protection obligations in the private sector. The data protection offence defined in Criminal Code, c 38 s 9 mostly applies to persons who are not acting as the controller or processor under data protection law. Of course, numerous types of criminal offences may still be committed by controllers, processors, and persons employed by them in connection with their activities related to personal data. See Data Protection Act, s 26(1), which references some applicable Criminal Code offences.

¹⁶⁵ Data Protection Act, s 22.

¹⁶⁶ Interview with Heikki Huhtiniemi, Senior Inspector, Office of the Data Protection Ombudsman (26.6.2024).

¹⁶⁷ See Data Protection Act, s 25.

¹⁶⁸ Interview with Heikki Huhtiniemi, Senior Inspector, Office of the Data Protection Ombudsman (26.6.2024).

¹⁶⁹ The Sanctions Board issued its first decisions on administrative fines under the GDPR in May 2020, and in 2020–2022, it issued a total of 17 administrative fines (*Annual Report of the Office of the Data Protection Ombudsman 2022*, Helsinki, Office of the Data Protection Ombudsman, 2023, online <https://tietosuoja.fi/documents/6927448/169954657/TSV+Annual+Report+2022.pdf>, p. 16). In addition to these, the reviewed decisions include four decisions from 2023, one decision from 2024, and one decision from 2021 where an administrative fine was not imposed. The decisions of the Sanctions Board, as well as a selection of other decisions by the Data Protection Ombudsman, are published at Finlex, ‘Tietosuojavaalututettu’ 2024 (last updated), online <https://www.finlex.fi/fi/viranomaiset/tsv>.

¹⁷⁰ Interview with Heikki Huhtiniemi, Senior Inspector, Office of the Data Protection Ombudsman (26.6.2024).

decisions on sanctions is typically gathered from the involved parties. Requests for information are usually sent only to the controller (or processor) under investigation, or persons or companies associated with them. However, in some cases, information has been requested also from third parties. In one decision, it is mentioned that information had been requested from a service provider, but the request had not been answered; the decision does not mention any further enforcement attempts.¹⁷¹ In at least two cases, the Deputy Data Protection Ombudsman had received subscriber identity information from telecommunications operators regarding telephone numbers.¹⁷² In a further case, information concerning the ownership of an internet domain name had been obtained from an official database maintained by Traficom.¹⁷³ The published decisions do not specifically name the legal bases for these requests (although the requests sent to the third parties presumably did), but all of these requests would seem to fall under Section 18(1) of the Data Protection Act.

3.2. Voluntary cooperation

There is no public information to support the existence of any voluntary cooperation between OSPs and Finnish administrative authorities in gathering electronic evidence for the purposes of punitive administrative proceedings. In the interviews conducted while preparing this national report, none of the interviewees (representing the Tax Administration, the FIN-FSA, the FCCA and the Office of the Data Protection Ombudsman) reported any voluntary cooperation practices with private third parties such as OSPs.¹⁷⁴

¹⁷¹ Decision of 26.5.2020, 8393/161/2019 (Taksi Helsinki Oy).

¹⁷² Decision of 23.7.2020, 3425/157/2019, 3578/157/2019, 3846/157/2019, 3871/157/2019, 3891/152/2019, 3918/157/2019, 4338/157/2019, 4666/154/2019, 5973/157/2019, 6773/157/2019 and 7022/157/2019 (Acc Consulting Varsinais-Suomi) and decision of 24.6.2021, 2890/161/2021 (XX Oy). Both cases concerned telemarketing. In the latter case, information had also been requested and received from a company that had provided telemarketing services as a subcontractor for the controller that was under investigation. This subcontractor was found to have been acting as a processor, despite the lack of a proper data processing contract referred to in GDPR, Article 28(3). The activities of the subcontractor were evaluated in a separate decision of the Sanctions Board, but no administrative fine was imposed on it (Decision of 24.6.2021, 2889/161/2021 (Y Oy)).

¹⁷³ Decision of 16.12.2021, 4282/161/2021 (Travel agency).

¹⁷⁴ The FCCA interviewees mentioned that some informal queries may also be made to foreign companies on a completely voluntary basis (e.g., via telephone), but this is done one a case-by-case basis and there are no established, continuous practices (interview with Vilhelmiina Ihamäki, Senior Adviser and Kalle Markkanen, Senior Specialist, Finnish Competition and Consumer Authority (25.6.2024)).

The interviewees generally highlighted that the gathering of information from third parties, including the gathering of evidence in punitive administrative proceedings, is strongly based on the law.

4. TRANSFER OF DATA BETWEEN PROCEEDINGS

4.1. Transfers of data between national proceedings

Transfers of evidence between different administrative and criminal enforcement authorities are governed by a complex web of interrelated provisions on rights to receive information, as well as rights and obligations to provide information. Administrative authorities typically have extensive rights to receive information that is necessary for the performance of their tasks and duties from each other, and to some extent also from criminal justice authorities. Such information can be provided on request, but authorities may also be allowed to disclose information on their own initiative.

The Customs Act does not contain provisions on information transfers between different public authorities, nor between administrative and criminal proceedings within the Customs. However, the Customs may obtain information from various databases and information systems maintained by public authorities (and some private entities) under the Act on the Processing of Personal Data in the Customs.¹⁷⁵ The data covered by Section 16 of this Act can be received directly via a technical interface or as a dataset, as agreed with the entity maintaining the database. Some of the data can only be obtained for the crime prevention tasks of the Customs,¹⁷⁶ whereas some can also be obtained for its other tasks as an administrative authority. However, in many cases, the data is also limited to specific information or data points contained in some information system. Consequently, Section 16 would not seem to be particularly relevant in enabling transfers of electronic evidence obtained from OSPs to punitive investigations in the field of customs enforcement. The same act also governs some transfers of personal data from the Customs to other public authorities, including (other) criminal justice authorities and the Tax Administration.¹⁷⁷ Further provisions regarding information transfers between the Customs and specific authorities are found elsewhere in legislation.

¹⁷⁵ *Laki henkilötietojen käsittelystä Tullissa*, 650/2019.

¹⁷⁶ Notably, Act on the Processing of Personal Data in the Customs, s 16(1)(14) contains a right to receive information from telecommunications operators. However, this point only concerns obtaining traffic data and location data for the purposes of crime prevention, and requires that the conditions for traffic data monitoring or obtaining location data are met. It does not enable requesting access to such data from telecommunications operators in administrative investigations.

¹⁷⁷ See Act on the Processing of Personal Data in the Customs, ss 20–26.

The Tax Administration has a general right to report suspected tax offences to the Police and/or to the Customs,¹⁷⁸ although in minor tax fraud and tax violation cases it may decide not to report the matter, also considering possible tax penalties.¹⁷⁹ Transfers of potential evidence and other information to the Tax Administration are in part covered by the general obligations applying to other public authorities. For example, the Customs has a general obligation to provide information related to VAT supervision to the Tax Administration,¹⁸⁰ but this mainly relates to information contained in customs declarations and customs clearance decisions and does not concern electronic evidence obtained from OSPs. The Act on the Assessment Procedure further contains a provision on the special obligation of public authorities to provide information to the Tax Administration on its request, which is applicable also in VAT enforcement,¹⁸¹ and may be used to request any sort of evidence relevant to a specific investigation. At least in theory, it could apply to evidence obtained from OSPs by other authorities. On the other hand, the Tax Administration may on its own initiative provide information contained in taxation documents to several other authorities – including the Police, the Customs, the FIN-FSA and the FCCA – under the Act on the Public Disclosure and Confidentiality of Tax Information¹⁸², Section 18.¹⁸³ The Tax Administration may also provide information to various authorities on request.¹⁸⁴

The FIN-FSA generally has an obligation to report suspected crimes to the competent criminal investigation authorities but may omit the notification in lesser cases where an administrative sanction is considered sufficient.¹⁸⁵ The FIN-FSA's rights to receive information from other public authorities are regulated in Chapter 3 of the FSA Act. More specifically, the FIN-FSA has a

¹⁷⁸ Act on the Tax Administration, s 28.

¹⁷⁹ Act on the Assessment Procedure of Self-assessed Taxes, s 76(2) and, for offences involving certain other taxes, Act on the Assessment Procedure, s 86(2).

¹⁸⁰ Act on the Assessment Procedure of Self-assessed Taxes, s 29(6). This information is provided daily via an electronic interface. The Customs has the competence to supervise the taxation of imported goods under VAT Act, Section 160. See also Act on the Processing of Personal Data in the Customs, s 21(1)(1).

¹⁸¹ Act on the Assessment Procedure, s 20, which is referenced in Act on the Assessment Procedure of Self-assessed Taxes, s 30(1).

¹⁸² *Laki verotustietojen julkisuudesta ja salassapidosta*, 1346/1999.

¹⁸³ On information exchange between the Customs and the Tax Administration in relation to VAT enforcement, see also VAT Act, s 160(3) and Act on the Public Disclosure and Confidentiality of Tax Information, s 18(1)(11).

¹⁸⁴ See Act on the Public Disclosure and Confidentiality of Tax Information, ss 19–20.

¹⁸⁵ See FSA Act, ss 3c(2) and 40(3). If the FIN-FSA does not have the investigatory powers or means required to investigate a potential violation that could be administratively sanctionable but also constitute a criminal offence, reporting the case to the criminal investigation authorities may be the only option (interview with Pia Ovaska, Chief Legal Advisor, Financial Supervisory Authority (13.6.2024)).

right to obtain information from the register of fines and the criminal record (Section 20), from criminal justice authorities in specific situations relating to cooperation obligations laid down in EU law (Section 20a), and generally from public authorities holding information needed for its supervisory tasks (Section 20b).¹⁸⁶ These provisions seem unlikely to apply to evidence originally obtained from OSPs in practice, but it is not impossible that Section 20a or 20b would enable transferring such evidence to the FIN-FSA under specific circumstances. Instead, the FIN-FSA's rights and obligations to provide information to criminal investigation authorities and administrative authorities that need it for their tasks are regulated in FSA Act, Section 71. In relation to some authorities, the purposes are specified broadly, whereas in regard to others, the purposes are limited to a specific task or context. If evidence obtained from an OSP by the FIN-FSA were needed by another authority mentioned in this provision, Section 71 might serve as a basis for a transfer in a specific case.

As regards the FCCA, the Competition Act contains rules on information transfers to and from criminal investigation authorities and prosecutors, as well as various other supervisory authorities including the FIN-FSA and Tax Administration. The key provision is Competition Act, Section 39. Subsection 1 provides that the FCCA may on its own initiative disclose information and documents, if this is necessary, to other authorities for purposes laid down in this provision. In relation to the criminal justice authorities and the Tax Administration, the purposes are specified broadly, but disclosure to the FIN-FSA is permitted for a more limited purpose (performing supervisory duties related to electricity and natural gas supply and derivative contracts).¹⁸⁷ Conversely, under Subsection 2, the FCCA has the right to receive from other authorities any information or documents necessary to establish whether an infringement concerning restrictions of competition or competition neutrality has occurred, and to control concentrations. Both subsections could theoretically serve as a basis for transfers of evidence originally obtained from OSPs, but their practical significance in this regard is unclear.

The Data Protection Act does not contain a specific provision regarding the Data Protection Ombudsman's right or duty to notify the Police of suspected criminal offences. However, in the government proposal on the Act, it is stated that a notification to the criminal investigation authorities is possible even without an explicit provision.¹⁸⁸ The Data Protection Act also

¹⁸⁶ FSA Act, ss 20, 20a and 20b.

¹⁸⁷ See also FSA Act, s 71(1)(11b).

¹⁸⁸ HE 9/2018 vp, p. 98. As noted in the government proposal, such a provision did exist in the preceding Personal Data Act (*henkilötietolaki*, 523/1999), s 40(1), but it was considered unnecessary in the new act. Cf. GDPR, Article 58(5).

does not explicitly regulate information transfers between domestic authorities, but the right to obtain information under Section 18(1) does not distinguish between private and public entities. Therefore, it covers also any public authorities that hold information necessary for the supervisory tasks of the Data Protection Ombudsman, potentially also applying to evidence originally obtained from OSPs by these other authorities. The Data Protection Act does not contain any provisions on information transfers from the Data Protection Ombudsman to other domestic authorities.

In summary, the rules on information transfers between public authorities typically do not differentiate between data categories, nor make any distinction in relation to how or from what source the information has been originally obtained. While some provisions limit the purposes for which information can be provided or obtained, or only concern transfers of information regarding specific issues, many provisions cover any relevant information needed by the authority in question. The rather general and abstract nature of these provisions makes it very difficult to enumerate all possible practical circumstances in which they may be applicable. Still, many of them potentially cover any data received from OSPs, as long as these are relevant for the performance of the tasks of the receiving authority, or the specific purposes defined in the provision in question. However, it should be highlighted that the web of provisions on rights to provide and obtain information of different public authorities is rather complex and contains many overlapping and interrelated provisions. Consequently, individual provisions do not necessarily constitute absolute rights, but may be subject to limitations specified in other legislation.

It should also be emphasised that there are some specific limits to transfers of evidence, in particular concerning transfers from criminal proceedings to administrative proceedings. Most importantly, in crime prevention and in criminal proceedings, electronic evidence may be gathered with invasive covert investigatory powers and coercive measures such as telecommunications interception, traffic data monitoring and technical surveillance. The use of such measures is subject to high material prerequisites (e.g., concerning the severity of the offence under investigation) and procedural safeguards (e.g., the requirement of a judicial warrant). While these measures may also yield evidence that is not connected to the suspected offence and might be useful in punitive administrative proceedings, the use of such ‘surplus information’ is strictly regulated. Any surplus information must be destroyed if it not usable for the purposes specifically allowed in the law,¹⁸⁹ which do not include use in punitive administrative proceedings.

¹⁸⁹ See Coercive Measures Act, c 10 ss 55–57; Police Act, c 5 ss 53–55; Act on Crime Prevention in the Customs, c 3 ss 52–54; Act on Crime Prevention by the Border Guard, ss 47–49.

4.2. Transfers of data between foreign and national proceedings

In relation to service providers outside Finnish jurisdiction, the primary means for gathering evidence are requests for administrative assistance addressed to the competent supervisory authorities, i.e., the foreign counterparts of the Finnish authorities in these sectors. Finnish parliamentary acts typically only regulate the disclosure of information to foreign authorities.¹⁹⁰ However, extensive cooperation, information exchange and mutual administrative assistance requirements concerning European supervisory authorities are contained in relevant EU legislative instruments, many of which are directly binding regulations. These instruments cover cooperation in all of the focus areas of this report.¹⁹¹

In addition to EU law, mutual administrative assistance can be based on international treaties. Possible legal bases for cooperation between tax authorities include the Convention on Mutual Administrative Assistance in Tax Matters (ETS No. 127) and bilateral tax treaties.¹⁹² In the area of data protection, cooperation with non-EU authorities can be based on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).¹⁹³ In regard to competition law, the Nordic Agreement on Cooperation in Competition Cases enables

¹⁹⁰ See, e.g., Act on the Openness of Government Activities, s 30; FSA Act, ss 52 and 71; Competition Act, s 40; Data Protection Act, s 18a.

¹⁹¹ See, e.g., Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, Article 4; UCC, Article 47; MAR, Articles 25 and 26; Benchmark Regulation, Article 39; Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, Article 12; GDPR, Article 61. Cooperation between authorities is also regulated in, e.g., ECN+ Directive, Article 24 and Law Enforcement Directive, Article 50. In the area of taxation, there are EU legislative instruments that are specifically focused on administrative cooperation and mutual assistance: Council Regulation (EU) No 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax; Council Directive 2010/24/EU of 16 March 2010 concerning mutual assistance for the recovery of claims relating to taxes, duties and other measures; Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EE (with its later amendments, including the aforementioned DAC7 Directive).

¹⁹² In more detail, see Tax Administration, 'International exchange of information on natural persons between tax authorities' 2024, online <https://www.vero.fi/en/detailed-guidance/guidance/75263/international-exchange-of-information-on-natural-persons-between-tax-authorities2/>.

¹⁹³ Mutual assistance is the subject of Chapter 4 (Articles 13–17) of the original Convention, and Chapter 5 (Articles 16–21) of the modernised version 'Convention 108+' (as amended by Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223)). On the domestic level, see Data Protection Act, s 18a.

cooperation between the competition authorities of Finland, Denmark, Iceland, Norway and Sweden.¹⁹⁴ In addition to the customs cooperation and administrative assistance agreements with third countries signed by the EU, Finland has made numerous bilateral agreements regarding cooperation in customs matters.

4.3. Admissibility of data collected from online service providers as evidence

In principle, any information that is transferred between authorities in accordance with the law is admissible in administrative proceedings and appeals thereof, as well as in criminal trials. Notably, even illegally obtained evidence may be admissible in the courts. As per Administrative Judicial Procedure Act, Section 83, an administrative court may not use evidence procured in violation of a statutory right or obligation to remain silent, or otherwise unlawfully, if such use jeopardises a fair trial. In considering whether the right to fair trial is jeopardised, the court must consider the nature of the matter, the severity of the violation of rights involved in procuring the evidence, the significance of the manner of procurement for the reliability of the evidence, the significance of the evidence for deciding the matter, and other circumstances. In particular, intentional illegal conduct by public officials, such as the deliberate misuse of investigatory powers (e.g., telecommunications interception, traffic data monitoring or technical surveillance) by criminal justice authorities with the purpose of transferring evidence to be used in punitive administrative proceedings where such investigatory measures cannot be used, would very likely render the proceedings unfair and therefore result in inadmissibility.

While there are no specific exclusionary rules in the Administrative Procedure Act or the sectorial legislative frameworks discussed in this report, and while a court may not pre-emptively order evidence to be excluded during an ongoing administrative investigation,¹⁹⁵ decisions on administrative sanctions should not be based on evidence that would be inadmissible in the subsequent appeal proceedings. As already mentioned, the party under investigation can present their view on the admissibility of any evidence already during the administrative proceedings.

As regards the general courts, there is a similar general exclusionary rule concerning illegally gathered evidence in Code of Judicial Procedure, Chapter 17, Section 25(3). Having been introduced in the evidence law renewal concerning general courts some years earlier,¹⁹⁶ it served as a model

¹⁹⁴ See Competition Act, ss 35(4), 36(2) and 40(2).

¹⁹⁵ Market Court Decision of 24.6.2024, MAO:375/2024.

¹⁹⁶ Amendment 732/2015, which entered into force on 1.1.2016.

for the aforementioned Administrative Judicial Procedure Act exclusionary rule.¹⁹⁷ However, the wording of the provision applicable in the general courts seems to set the admissibility of illegally obtained evidence as the default option: the court *may use* also evidence that has been obtained unlawfully, *unless* such use would endanger the conduct of fair proceedings (having regard to the same criteria that are mentioned in the Administrative Judicial Procedure Act provision). It is debatable to what extent this inversion of the wording (which was proposed during the parliamentary proceedings by the Legal Affairs Committee in order to highlight that exclusion of evidence should be a rare exception)¹⁹⁸ actually lowers the bar of admissibility. In any case, illegal evidence-gathering practices intentionally employed by public officials during punitive administrative proceedings would typically render evidence so obtained inadmissible in criminal trials, as well.

These exclusionary rules also cover, in a similar fashion, evidence obtained unlawfully by foreign authorities. If electronic evidence is gathered from OSPs (or otherwise) in violation of Finnish law by foreign authorities and then subsequently transferred to be used in Finnish administrative or criminal proceedings, the admissibility of this evidence must be evaluated on a case-by-case basis under the criteria specified in the aforementioned exclusionary rule provisions. However, it is worth noting that in a notable criminal case, the Supreme Court did not exclude messages acquired by the Federal Bureau of Investigation (FBI) from the smartphone-based ANOM messaging platform in the international sting operation ‘Trojan Shield’¹⁹⁹ despite finding them unlawfully obtained. In this case, although the initial gathering of the messages was unlawful (as there was no legal basis in Finnish law for the operation, and the gathering targeted users of ANOM devices

¹⁹⁷ In the government proposal, Administrative Judicial Procedure Act, s 83 was described as corresponding to the key principles of the Code of Judicial Procedure provisions on exclusionary rules (HE 29/2018 vp, p. 151).

¹⁹⁸ See HE 46/2014 vp, pp. 92–95 and LaVM 19/2014 vp, pp. 7–8.

¹⁹⁹ The ANOM platform, consisting of specifically modified devices and a messaging app, was marketed specifically to criminals as a means for secure encrypted communications. In reality, the devices were covertly distributed by law enforcement agencies, who also operated the messaging service and monitored all communications. The operation has been designated ‘Greenlight’ by the Europol and ‘Ironside’ by the Australian Federal Police. See United States Department of Justice, ‘FBI’s Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown’ 2021, online <https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive>; Europol, ‘800 criminals arrested in biggest ever law enforcement operation against encrypted communication’ 2021, online <https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication>; Australian Federal Police, ‘AFP-led Operation Ironside smashes organised crime’ 2021, online <https://www.afp.gov.au/news-centre/media-release/afp-led-operation-ironside-smashes-organised-crime>.

located in Finland), the evidence was later transferred to the Finnish authorities through proper channels and procedures. Importantly, the initiative to the unlawful sting operation did not come from the Finnish authorities.²⁰⁰

Prior to the enactment of the Administrative Judicial Procedure Act, the Supreme Administrative Court had accepted the use of illegally obtained evidence in punitive tax proceedings in a case related to the so-called 2008 Liechtenstein tax affair.²⁰¹ The evidence that was deemed admissible had been originally obtained (possibly illegally) by an employee of a Liechtenstein-based bank and sold to the German Federal Intelligence Service (*Bundesnachrichtendienst*), who had then handed the material over to the German tax authorities. Further copies had been distributed to tax authorities in other countries, and some of these files had eventually been obtained by the Tax Administration via a legal assistance request from Australian tax authorities.

It is noteworthy that in the committee report discussing the Code of Judicial Procedure exclusionary rule (which, as mentioned, later served as a model for Administrative Judicial Procedure Act, Section 83), the Legal Affairs Committee stated that a criminal offence committed by a private party, such as a bank employee, should lead to the exclusion of evidence so obtained only in very exceptional cases.²⁰² In light of this, it could be interpreted that despite the new provisions, evidence obtained in a way corresponding to the Liechtenstein tax affair would still likely be admissible in criminal proceedings as well as in punitive tax proceedings and appeals thereof. In contrast, it has been established already in earlier case law that information received through mutual legal assistance solely for the purpose of being used in criminal proceedings cannot be used in taxation,²⁰³ or in punitive administrative proceedings in violation of such restrictions of use.²⁰⁴

²⁰⁰ ECLI:FI:KKO:2023:14. Concerning this case and the meaning of ‘unlawful’ or ‘illegal’ in a cross-border law enforcement context, see also J. Riekkinen, ‘Unlawfully Obtained Evidence, Cross-Border Law Enforcement Operations and Borderless Networks’ *Jusletter IT*, 2023, DOI:10.38023/7091c0c1-db24-4fcb-a61d-ac5098ac3fd7.

²⁰¹ ECLI:FI:KHO:2016:100. While the particular case concerned income taxes, there is no reason to assume that the assessment of the Supreme Administrative Court would have been any different in a VAT enforcement case.

²⁰² LaVM 19/2014 vp, p. 21 (further mentioning the specific scenario in which ‘bank account information stolen from a foreign bank comes into the possession of Finnish tax authorities’, in an obvious reference to the Liechtenstein tax affair).

²⁰³ Supreme Administrative Court, ECLI:FI:KHO:2000:61.

²⁰⁴ In the Supreme Court case ECLI:FI:KKO:2006:11, four officials of the Tax Administration were convicted for violation of official duty because they had used information received from abroad in a tax audit report, although the use of this information for taxation purposes had been forbidden by the Luxembourg authorities that had supplied it in response to a mutual legal assistance request. Restrictions set by the assisting country are

Additionally, in criminal proceedings, evidence that has been obtained in administrative proceedings contrary to the privilege against self-incrimination may be excluded under Code of Judicial Procedure, Chapter 17, Section 25(2).²⁰⁵ This subsection prohibits the use of evidence obtained from a person in proceedings other than a pre-trial investigation or in criminal proceedings, through a threat of coercive measures or otherwise against their will, if they at the time were a suspect or defendant of an offence or if a pre-trial investigation or proceedings were underway for an offence for which they were charged, and if the obtaining of the evidence would have been contrary to the right not to testify in a trial.²⁰⁶ As has been discussed above, in punitive administrative proceedings, a third party typically cannot be ordered to provide information if they have a right not to testify, or issued a coercive fine to enforce an obligation to provide information if there is a reason to suspect this person of a criminal offence. Like other rules concerning the privilege against self-incrimination, this exclusionary rule is typically not relevant in situations where evidence has been requested from an OSP.

5. CONCLUSION

The gathering of electronic evidence from OSPs has not been specifically addressed by the Finnish legislator in the context of punitive administrative proceedings. However, the administrative authorities in the areas of customs, taxation, banking and financial markets, competition and data protection have broad general legal bases that empower them to request and receive information from various sources, including private third parties that may hold evidence that is relevant in administrative investigations and in imposing punitive administrative sanctions. While these rights to receive or obligations to provide information could be interpreted to form legal bases for requests concerning various categories of electronic evidence held by different kinds of OSPs, it would seem that in practice, such requests are not very common. Beyond requests based on the law, none of the authorities in these sectors are known to have any voluntary cooperation practices that enable them to receive electronic evidence from OSPs.

While the provisions that enable different authorities to request information needed in punitive (and other) administrative proceedings from third parties generally resemble each other, there are some differences in their exact wordings, limitations and level of detail. In general, these provisions

binding under Act on International Legal Assistance in Criminal Matters (*laki kansainvälisestä oikeusavusta rikosasioissa*, 4/1994), s 27(2).

²⁰⁵ In contrast, sub-ss 1 (concerning evidence that has been obtained through torture) and 3 apply in both criminal and civil proceedings in the general courts.

²⁰⁶ See Code of Judicial Procedure, c 17 s 18.

are considerably less precise and include fewer procedural and material safeguards than the legislation concerning the investigatory powers of the criminal justice authorities. In order to define the practical limits of these powers, the authorities themselves must carefully consider whether information held by a third party is in fact relevant and needed in their investigation, and whether obligating the third party to provide it would be proportionate.²⁰⁷ Furthermore, constitutional limits must also be considered: for instance, while none of the provisions specifically exclude requesting communications content or metadata directly from communications services providers, this would very likely not be acceptable or lawful from a constitutional point of view. In practice, the authorities do not seem to make such requests to communications intermediaries based on these provisions. In relation to requests for subscriber information, the interpretations of different authorities appear to diverge from each other. It might therefore be beneficial to introduce more precise provisions concerning requests for subscriber information to the acts governing the powers of these authorities.

As an enforcement measure, in most cases the competent authorities in the aforementioned areas may impose, and order payable, coercive fines on those who refuse to provide information on request. However, in practice, coercive fines are very rarely imposed on third parties. In tax enforcement and competition law enforcement, the failure to fulfil an obligation to provide information may be administratively sanctionable in itself, but these sanctions are likewise rarely utilised. No other enforcement measures seem to be used against third parties. However, it is worth noting that all of these authorities have the right to receive executive assistance from the Police in completing their tasks and duties.²⁰⁸ The possibility of relying on executive assistance by the Police in realising the right to information (i.e., the use of force to physically gain access to documents or devices in the possession of third parties) has been suggested in literature²⁰⁹ and discussed within some authorities.²¹⁰

²⁰⁷ Proportionality in relation to the objectives pursued is one of the principles of good administration established in Administrative Procedure Act, s 6. The evaluation of necessity was generally highlighted by the interviewees representing different authorities.

²⁰⁸ Customs Act, s 101; Act on the Assessment Procedure of Self-assessed Taxes, s 79; Act on the Assessment Procedure, s 93; FSA Act, s 25a; Data Protection Act, s 20. These provisions do not limit or specify the tasks or duties for which executive assistance may be given. As regards the FCCA, the Police may provide assistance in on-site inspections under Competition Act, s 37(5) and Police Act, c 9 s 1 (as well as FCCA Act, s 7b(2) and 7e(2)).

²⁰⁹ Rabinä, (n. 79), p. 627.

²¹⁰ The possibility of requesting executive assistance from the Police has been subject to some internal discussions in the Tax Administration (interview with Sami Peltola, Compliance Manager, Tax Administration (24.6.2024)). Executive assistance was mentioned as a possible option in non-compliance situations also in the interview with Heikki Huhtiniemi, Senior

The initial request for information may be relatively informal and typically does not constitute an appealable administrative decision. In the context of tax enforcement, such a decision must be made when a third party refuses to obey the request, but other sector-specific laws do not have similar provisions regarding administrative decisions and the right to appeal in these situations. Hence, there is some room for interpretation on whether requests, orders or other documents establishing and specifying the obligation to provide information may (or should) constitute appealable administrative decisions as such when not enforced with a coercive fine. The prevailing interpretation seems to be that they do not. However, decisions on coercive fines as an enforcement measure or sanctions for non-compliance can always be appealed in court by the obligated or sanctioned third party. Other than that, the law usually does not define specific safeguards and remedies for the third party that is subjected to such a request.²¹¹ Instead, for the entity under investigation, challenging the admissibility of the evidence received from a third party (during the administrative proceedings and in subsequent appeal proceedings) seems to be the primary available remedy, as the general or sectorial frameworks do not contain any specific *ex ante* remedies in regard to evidence-gathering from third parties.²¹²

Existing legislation generally allows for various kinds of information to be transferred between different authorities that may impose punitive administrative sanctions, as well as between administrative authorities and criminal investigation authorities. Under specific circumstances, this may potentially also include electronic evidence obtained from OSPs. As an exception, information produced as ‘surplus information’ with covert investigatory powers or coercive measures employed by criminal justice authorities cannot be used in punitive administrative proceedings. Electronic

Inspector, Office of the Data Protection Ombudsman (26.6.2024), but in practice, it has not been relied on.

²¹¹ However, general safeguards and remedies in public administration are typically available. These include, e.g., administrative complaints under Administrative Procedure Act, c 8a, complaints to the Chancellor of Justice and the Parliamentary Ombudsman, and criminal and civil liability of public officials.

²¹² Additionally, in some situations, interim measures can be sought by third parties obligated to provide information or the suspected entity. See Administrative Judicial Procedure Act, s 123. According to sub-s 1, while an appeal is pending, an administrative court may prohibit enforcement of a decision, order suspension of enforcement, or issue some other order concerning enforcement of a decision. Under sub-s 2, an administrative court may also issue an interim order safeguarding the exercise of the rights or interests of a party in an administrative judicial matter that the court is considering other than an appeal. In some situations, administrative authorities can order that their decision shall be complied with regardless of appeal, unless the appellate authority orders otherwise. E.g., according to Competition Act, s 49a(1), this possibility specifically applies to decisions on requests to provide information under s 33.

evidence originating from requests directed at OSPs that has been transferred from one authority to another is generally admissible in both administrative proceedings and criminal trials, unless the evidence in question has been obtained unlawfully and its use would endanger the right to fair trial. Possible exclusion of evidence is subject to case-by-case analysis based on criteria defined in the law. This also applies to evidence unlawfully gathered by foreign criminal justice or administrative authorities.

6. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN FRANCE

M. LASSALLE

1. COMPETENT AUTHORITIES IN SELECTED AREAS OF PUNITIVE ADMINISTRATIVE ENFORCEMENT

Several administrative bodies are covered in this study.

French customs are an administrative body. Some of its agents, reporting to the Ministry of Economy and Finance, while not involved in standard criminal investigations, still possess investigative powers to detect illegal activities. This enforcement model is unique among the other punitive administration enforcement models addressed in this chapter. As a matter of facts, the Customs Code (*Code des douanes*), which is the legal basis for their activities and powers, does not mention administrative offences (*sanctions administratives*). Only customs criminal offences are mentioned (*contraventions douanières*).¹ Although customs criminal offences belong to the formal category of criminal offences, the detection and investigation of these offences is entrusted to an administration and not to the judicial police and will therefore be addressed in this chapter.

In the area of tax law enforcement, there are agents within the tax administration, reporting to the French Ministry of Economy and Finance, who are not involved in criminal investigations but hold investigative powers to detect and punish administrative offences. These activities and powers are based on the General Tax Code (*Code Général des Impôts*) and the Tax Procedures Book (*Livre des procédures fiscales*), and they will be the subject of study in this chapter.

In the area of banking and financial law, two authorities are particularly relevant. The Prudential Control and Resolution Authority (*Autorité de Contrôle Prudentiel et de Résolution*, ACPR) is responsible for the administrative oversight of credit institutions, particularly in relation to their prudential obligations and preventative measures against money laundering

¹ Article 408 to 440 of the Customs Code. See also R. Cren, *Poursuites et sanctions en droit pénal douanier*, Paris, France, Panthéon Assas University, 2011, online <https://docassas.u-paris2.fr/nuxeo/site/esupversions/856c3295-7d96-422f-b3e0-24dfc799fcf7?inline>, p. 20.

and terrorist financing. Although it is entrusted with financial autonomy, it does not belong to the category of independent administrative authorities since 2017, and reports to the French central bank.² Meanwhile, the Financial Markets Authority (*Autorité des Marchés Financiers*, AMF) supervises other financial institutions. It belongs to the category of independent public authorities.³ Both authorities have powers of punitive administrative enforcement, based on the administrative offences listed in the Financial and Monetary Code (*Code Monétaire et Financier*).

The competition authority (*Autorité de la Concurrence*) is the principal administrative body responsible for overseeing administrative policing in the field of competition law.⁴ It is an independent administrative authority, and its organisation and powers are based on the Commercial Code (*Code du Commerce*).⁵

Finally, the French data protection authority (*Commission Nationale Informatique et Liberté*, CNIL) oversees the enforcement of data protection law. It is an independent administrative authority, and its organisation and powers are not codified, but based on a self-standing act.⁶

One should add that, certain services of the tax and customs administrations may be granted judicial police powers.⁷ In such cases, they operate under the Code of Criminal Procedure (*Code de Procédure Pénale*), and the exercise of these powers falls within the area of the judicial police.⁸ They will apply the powers entrusted to the judicial police, including those related to production orders targeting OSPs.⁹

2. PUNITIVE ADMINISTRATIVE PROCEEDINGS: GENERAL FRAMEWORK

It is important to clarify from the outset that there is no general framework in France regarding punitive administrative investigations. Historically, investigative measures specific to administrative authorities have been developed following a sectorial approach rather than a global one, which explains the existence of sectorial frameworks that are not coordinated

² Article L 612-1 of the Financial and Monetary Code.

³ Article L 621-1 of the Financial and Monetary Code.

⁴ It is not the only authority in charge of administrative policing regarding competition law. Specialised regional authorities are also entrusted with a part of this mission.

⁵ Article L 461-1 of the Commercial Code.

⁶ Article 8 Law no. 78-17 of 06.01.1978 Law no. 2004-575 of 21.06.2004 on Information Technology, Files and Freedoms, the French Data Protection Act (*Loi relative à l'informatique, aux fichiers et aux libertés*).

⁷ See in particular the National Anti-Fraud Office (*Office National Antifraude*, ONAF), replacing the former Financial Investigation Service (*Service d'Enquêtes Judiciaires des Finances*) regarding tax and customs enforcement.

⁸ See article 28 to 28-3 of the Code of Criminal Procedure.

⁹ See, in particular, Article 60-1 to 60-3 of the Criminal Procedure Code.

with each other.¹⁰ However, there are general principles applicable to administrative investigations, which derive, in particular, from the application of fundamental rights. Despite the absence of systematisation by law or doctrine of general principles, it can be noted that the principle of legality appears to be considered as the main standard governing administrative investigations.¹¹

In practice, privacy and data protection are the most important fundamental rights that have, in recent years, contributed to reshaping the legal framework governing administrative investigations. This will be further developed in the following paragraphs.

With regard to the collection of data from online service providers (OSPs), it is worth noting that there has been a general trend towards change in recent years. Indeed, since the Digital Rights Ireland case of the European Court of Justice (ECJ),¹² the constitutional framework applicable to all the studied administrative measures, as well as to criminal investigations, has evolved.¹³ These changes are however very narrow as they were exclusively related to access to telecommunication metadata. The powers of numerous authorities capable of carrying out administrative investigations and imposing administrative sanctions have been affected. In all cases, the French Constitutional Council has (temporarily) stroke down legal bases available to different administrative authorities, including some of those covered by this study: the competition authority,¹⁴ the AMF,¹⁵ the High Authority for the Transparency of Public Life (*Haute autorité pour la transparence de la vie publique*),¹⁶ the customs administration,¹⁷ the administration in charge of controlling the legality of claims for social benefits¹⁸ and the administration in charge of intellectual property (HADOPI).¹⁹ As a consequence, most sectorial legal frameworks distinguish two sets of provisions: a general

¹⁰ H. Matsopoulou, 'De la preuve administrative à la preuve pénale', in: P. Beauvais, R. Parizot (eds.), *Les transformations de la preuve pénale*, Paris, LGDJ, 2018, pp 163-176.

¹¹ The principle of fairness is also mentioned, but its scope in the context of administrative investigations remains uncertain, as well as its place alongside the principle of legality, C. Testard. 'La loyauté de l'enquête administrative : les détours d'une évidence', *La Revue du Centre Michel de l'Hospital*, 2024, n° 27. See also, with a sectoral approach, N. Ida, *La preuve devant l'autorité des marchés financiers*, Paris, Dalloz, 2022, p. 346.

¹² ECJ, *Digital Rights Ireland*, 08.04.2014, Case C-293/12.

¹³ M. Lassalle, 'Enquêtes administratives et protection des données personnelles : les limites de la jurisprudence constitutionnelle', *Recueil Dalloz*, 2020, p. 68.

¹⁴ Conseil constitutionnel, 05.08.2015, 2015-715 DC, § 137.

¹⁵ Conseil constitutionnel, 21.07.2017, 2017-646/647 QPC, § 9.

¹⁶ Conseil constitutionnel, 08.09.2017, 2017-752 DC, § 83.

¹⁷ Conseil constitutionnel, 15.02.2019, 2018-764 QPC, § 8.

¹⁸ Conseil constitutionnel, 14.06.2019, 2019-789 QPC.

¹⁹ Conseil constitutionnel, 20.05.2020, 2020-841 QPC. See also ECJ, *La Quadrature du Net II*, 30/04/2024, C-470/21.

provision related to access to data in general²⁰ and a special provision related to access to telecommunications metadata. The purpose of the latter is to be more protective than the former, to match the requirements of the Constitutional Council (*Conseil constitutionnel*) and (partly) the requirements of the ECJ.

All these cases concerned access to telecommunication metadata (so-called *données de connexion*). In other words, there is a clear trend regarding access to this data in the context of administrative investigations. However, such a trend does not extend to other categories of data. This has two consequences. The Constitutional Council, like the ECJ, has not addressed other measures related to administrative investigations, including those involving cooperation with OSPs. In fact, the Constitutional Council has only ruled in one case involving a different type of data held by service providers other than OSPs, on access to banking data in an administrative context. It chose to clarify the distinction between the two types of data (bank data and telecommunication metadata).²¹ Even if bank data is highly sensitive,²² it is also deemed very ‘useful’ in the context in which the case was dealt with (i.e., social security investigations).²³ The reasoning used by the Constitutional Council to distinguish between the two categories of data is nonetheless questionable. The Council considers that bank data is just as sensitive as telecommunication metadata but is more “useful” in the context of the specific kind of administrative investigation that was at stake in that case. It means that the two categories cannot be clearly distinguished.²⁴

Considering this very specific trend in the French legal framework, there is another preliminary general element that should be considered. In all the cases where there are specific rules regarding a specific category of OSPs, the provisions refer to metadata data (*données de connexion*) that is subject to collection and retention obligations.²⁵ It seemingly excludes data that are processed on other bases than these legal obligations, and this data could be accessed on the basis of other investigative powers entrusted to the administrative authorities. There is therefore a common frame of reference that should be considered for all access measures by administrative

²⁰ In a few cases, there are several texts regulating cooperation with different kinds of addressees.

²¹ Conseil constitutionnel, 20.05.2020, 2020-841 QPC.

²² Conseil constitutionnel, 14.06.2019, commentary on decision 2019-789 QPC, p. 22.

²³ Conseil constitutionnel, 14.06.2019, commentary on decision 2019-789 QPC, p. 23.

²⁴ M. Lassalle, 'Enquêtes administratives et protection des données personnelles : les limites de la jurisprudence constitutionnelle', *Recueil Dalloz*, 2020, p. 68.

²⁵ These texts systematically refer to ‘The data retained and processed by electronic communications operators and the service providers mentioned in points 1 and 2 of I of Article 6 of Law No. 2004-575 of June 21, 2004, on confidence in the digital economy’. See sections 3.1.1, 3.1.2, 3.1.3 and 3.1.4.

authorities, even though it is not a general framework dedicated to administrative investigations.

This common framework is useful to understand the categorisation of data, which follows the ECJ's case law and should be at least partly common to other EU Member States.²⁶ These obligations apply to two categories of OSPs. The first category is that of electronic communications operators under Article L 34-1 of the French Post and Electronic Communications Code. However, this text does not define electronic communications operators, as it only refers to data retention obligations. The Code defines elsewhere an operator as 'any natural or legal person operating an electronic communications network open to the public or providing an electronic communications service to the public'.²⁷ The same Code defines electronic communications as 'the emission, transmission or reception of signs, signals, writing, images or sounds by cable, radio, optical or other electromagnetic means'.²⁸

The second category of actor is that of service providers mentioned in Articles 6 I 1 and 2 of Law no. 2004-575 on confidence in the digital economy, which are 'persons whose business is to provide access to online public communication services'²⁹ as well as 'persons who, even free of charge, make available to the public via online public communication services, the storage of signals, writings, images, sounds or messages of any kind supplied by recipients of these services'.³⁰ Data collected by service providers mentioned in Articles 6 I 1 and 2 of Law no. 2004-575 are not further defined, in that law, but in an administrative act.

For the sake of conciseness, the regulation of data, depending on their categorisation, applicable to both types of OSPs, is summarised in an annexed table at the end of this chapter.

Since data retention obligations constitute the only common basis across different sectors for administrative investigations, these obligations could attempt to define the territorial scope of administrative investigative powers. Yet, the law on data retention does not have a precise definition of their territorial scope.³¹

²⁶ The case *La Quadrature du Net II* did not change this categorisation.

²⁷ Article L 32 15° of the Post and Electronic Communications Code.

²⁸ Article L 32 1° of the Post and Electronic Communications Code.

²⁹ Article 6 I 1 of Law no. 2004-575 of 21.06.2004 on confidence in the digital economy (*Loi pour la confiance dans l'économie numérique*).

³⁰ Article 6 I 2 of Law no. 2004-575 on confidence in the digital economy.

³¹ Interestingly the territorial approach is clearer regarding the obligations to prevent hate speech for instance, see Article 6-4 of Law no. 2004-575.

3. PUNITIVE ADMINISTRATIVE PROCEEDINGS: SECTORIAL FRAMEWORK

In general, two forms of access to data held by OSPs can be distinguished. On the one hand, there are provisions specifying the modalities for accessing telecommunication metadata. On the other hand, there are general bases allowing access to data or information broadly understood. Depending on the situation, this second legal basis may take the form of general production orders, which can be directed at different kinds of OSPs for data other than metadata, or a much broader power of administrative search.

The issue of voluntary cooperation has not been subject to legislative or research developments in the context of administrative investigations. This issue has not received sustained attention in criminal procedure either. In the latter context, the matter has been scarcely addressed by the literature, and the Court of Cassation (*Cour de Cassation*) has fully validated, without any reservations, the practices of voluntary cooperation between French authorities and OSPs located abroad, in criminal proceedings.³² Similarly, the extraterritorial reach of production order has never been the subject to legislative or research developments in the context of administrative investigations.³³

3.1. Specific requests for data to online service providers

3.1.1. Customs enforcement

The specific legal basis to obtain data in customs administrative investigation covers the two categories of OSPs abovementioned.³⁴

The nature of the data which can be requested is not defined in that specific law; yet, it refers to Article L 34-1 of the Post and Electronic Communications Code and Articles 6 I 1 and 2 of Law no. 2004-575,

³² Cour de cassation, Chambre criminelle, 06.11.2013, 12-87.130. P. De Combles de Nayves, 'Réquisitions sans frontières', *Actualité Juridique Pénale*, 2014, p. 40. For a critical approach, see M. Lassalle, *L'accès transnational aux données bancaires dans le cadre de l'enquête pénale*, Bruxelles, Larcier, Collection de la faculté de Droit, d'Economie et de Finance de l'Université du Luxembourg, 2021; M. Lassalle, 'Transnational Public-Private Cooperation in a Repressive Context Understanding the Legal Framework for EU-U.S. Transfers of Financial Data', in: B. Vogel, E. Kosta, M. Lassalle (eds.), *Public-Private Information Sharing in the Fight against Money Laundering and Terrorism Financing*, Cambridge, Intersentia, 2024.

³³ See however, criticising the absence of such extraterritorial reach, M. Bouvard, T. Carcenac, J. Chiron, P. Dallier, J. Genest, B. Lalande and A. de Montgolfier, *Le e-commerce : propositions pour une TVA payée à la source*, Parliamentary Information Report, no. 691 (2014-2015), French Senate, 2015, p 10 and 41.

³⁴ Article 65 quinquies of the Customs Code.

meaning, to data retention obligations, which only covers telecommunication metadata.

Although this is a specific text that was meant to be more protective than general investigative powers, there are no substantial conditions to request the data. However, there is a limit regarding the purposes of the request. It should be undertaken for the purposes of establishing a limited number of customs criminal offences: aggravated smuggling,³⁵ intentional smuggling and customs fraud,³⁶ smuggling and customs fraud related to illicit financial transfers³⁷ and violation of foreign financial relations legislation.³⁸ The goal of the measure must be ‘gathering evidence and tracking down the perpetrators, accomplices and those who have participated as interested parties’.³⁹

The legal basis adds that ‘a decree issued after consultation with the Council of State [*Conseil d’Etat*] shall set out the terms and conditions for the application of the present article’, which should have clarified the rules of transfer of data. It seems however that this decree has not been adopted. The legal basis only states that ‘the data communicated is destroyed when the action for the application of tax penalties is terminated’.

Any refusal to provide the information or documents requested is punishable by a criminal fine of 3.700 euros.⁴⁰ Moreover, ‘offenders must be ordered to produce the books, records or documents that have not been disclosed, subject to a penalty of at least 150 euros for each day’s delay’.⁴¹

Before the aforementioned intervention of the Constitutional Council, a judicial authorisation was not requested.⁴² That decision of the Constitutional Council triggered a legislative reform requiring a specific procedure for the authorisation and control of those requests, based on the requirement of an authorisation by a judge or an independent body from the case law of the ECJ. The use of this power shall be previously authorised by the public prosecutor of the judicial court.⁴³ Moreover, ‘the public

³⁵ Article 414 of the Customs Code.

³⁶ Article 414-2 of the Customs Code.

³⁷ Article 415 of the Customs Code.

³⁸ Article 459 of the Customs Code.

³⁹ Anyone who, in any way, has participated in the offences mentioned in Articles 414, 414-2, and 415 of the Customs Code, is subject to the same penalties as the primary offenders, including those who have a direct interest in the fraud, cooperated in a collective fraudulent plan, or knowingly concealed the actions of the offenders or attempted to secure their impunity.

⁴⁰ Article 413 bis 2° § 2 of the Customs Code.

⁴¹ Article 431 of the Customs Code.

⁴² Conseil constitutionnel, 05.08.2015, 2015-715 DC, § 137.

⁴³ The public prosecutor’s authorisation, which may be given by any means, shall be mentioned or placed in the case file, Article 65 quinquies § 2 of the Customs Code.

prosecutor's authorisation, which may be given by any means, shall be mentioned or placed in the case file' and 'communication of the data referred to in the first paragraph is recorded in an official report, which is added to the case file. A copy of this report is sent to the public prosecutor who authorised the [measure] as well as to the operators and service providers [...], at the latest within five days of it being drawn up'.

Although this legal basis was meant to address the requirements of the ECJ, there are no direct remedies for the persons concerned by those requests. The legality of investigative measures can only be challenged if they are used as evidence in subsequent criminal or administrative proceedings. In other words, the interests of the data subjects are hardly taken into consideration. Notably, there are no remedies available to the OSPs either.

3.1.2. Tax enforcement as regards VAT

The legal framework applicable to the access of data held by OSPs by the tax administration is, like most other sectors, divided into several subcategories of investigative powers. The first subcategory concerns access to telecommunication metadata held by certain OSPs.⁴⁴ This special subcategory has been separated from other subcategories applicable to different private actors holding information. These other powers still exist, are very loosely regulated, and are excluded from this study as they do not apply to OSPs.⁴⁵ It is the category related to searches conducted by the tax administration that seems to be the only means available to access other categories of data held by OSPs.

The same OSPs as previously mentioned are covered, namely electronic communications operators, and service providers (see Section 2). Any data stored and processed by these OSPs in compliance with their data retention obligations can be accessed based on this special provision.

These data can be requested for the purposes of investigating or ascertaining certain aggravated administrative offences, including that of failure or delay in filing returns (such as VAT returns)⁴⁶ and underreporting.⁴⁷

⁴⁴ Article L 96 G of the Tax Procedures Book. One should mention that, based on Article L 82 AA of the Tax Procedures Book, the tax administration can access data processed by platform operators, when this data is related to the activities mentioned in Article 242 bis.

⁴⁵ See Article L 82 A to Article L 96 K of the Tax Procedures Book.

⁴⁶ Article 1728 1 c) of the General Tax Code.

⁴⁷ Such as inaccuracies or omissions in a declaration or document containing information to be taken into account for the assessment or liquidation of tax as well as the restitution of a tax claim the payment of which has been unduly obtained from the State (b and c of Article 1729). See also Article 1729-0 A I of the General Tax Code.

An administrative act codified the rules related to production order of telecommunication data in a dedicated part of the Tax Procedures Book.⁴⁸ According to Article R 96 G 2, ‘the request for authorisation to disclose telecommunication data shall specify: 1° The requesting department; 2° The name(s) of the person(s) for whom communication of telecommunication data is requested, or any information enabling them to be identified; 3° The connection data or types of telecommunication data requested for each person mentioned in 2°; 4° The periods for which this data is requested; 5° The factual and legal grounds for the request. If necessary, additional requests may be submitted in respect of proceedings for which a request has already been made’. According to Article R 96 G 5, this procedure is undertaken ‘by means of a written request for the authorisation of the controller of requests for telecommunication data’, and this request includes the aforementioned information except the identification of the requesting department. The addressee of the request ‘shall provide the data to the administration in electronic form, using a secure system’. Article R 96 G 6 adds that the data, once transmitted by the addressee of the request, ‘are collected and stored, until they are destroyed, in accordance with procedures designed to guarantee their confidentiality’. Article L 96 states the requirements regarding the destruction of the data. In general, data is destroyed after a period of one year from its receipt. There is an exception when the data is used in the context of a subsequent procedure, in such case they are destroyed upon expiry of all avenues of appeal. The directors (or their deputy) of the services who have resorted to such production order send a report to the controller of telecommunication data requests each year. This report also indicates the collected telecommunication metadata that have been destroyed.⁴⁹

Article 1734 of the General Tax Code provides for a penalty in case of refusal to provide the documents and information requested by the tax administration, which also extends to any behaviour that hinders disclosure, namely a criminal fine of 10.000 euros. It applies for each request if all or some of the documents or information requested are not provided. Similarly, a fine of the same amount is applicable if the documents are not kept or are destroyed before the prescribed deadline, in other words if data retention obligations are not respected.

Following the case law of the Constitutional Council and the ECJ, the main specificity of this article is the authorisation procedure. The legal basis

⁴⁸ Decree no. 2023-674 of 27.07.2023 regarding the procedure for the communication of connection data to tax administration officers, as provided for in Article L 96 G of the Tax Procedures Book (*Décret relatif à la procédure de communication des données de connexion aux agents de l'administration des impôts prévue à l'article L 96 G du livre des procédures fiscales*).

⁴⁹ Article R 96 G-7 of the Tax Procedures Book.

distinguishes internal and external authorisation. The former is entrusted to tax administration officials with at least the rank of controller and specially authorised by the director of the department to which they are assigned or their deputy.⁵⁰ Such power is carried out ‘by permanent civil servants belonging to category A or B bodies, authorised for this purpose by the director, or their deputy, in charge, as appropriate, of a regional or departmental public finance directorate, a service with national competence or a specialised tax audit directorate, in which these civil servants are assigned’.⁵¹

The external authorisation requires access to data to be subject to prior authorisation by a dedicated authority, namely the ‘controller of telecommunication data requests’,⁵² who verifies if the measure is justified. Therefore, production orders are referred to this controller in a reasoned request from the director or deputy director of the department seeking the data and must include all information required to justify the procedure. The authorisation is added to the procedure file.⁵³

This new authority is composed of two persons, namely the controller and their deputy. They are elected for a non-renewable term of four years. This article specifies the polls from where these persons are elected. As far as the controller is concerned, the position alternates between an active or honorary member of the Council of State (the highest administrative court), elected by the general assembly of the Council of State, and an active or honorary magistrate of the Court of cassation (the highest judicial court) elected by the general assembly of the Court of cassation. The provisions adds that a deputy from the other jurisdiction is appointed in the same way, so that there are always two members, representing both courts.

The controller is independent and ‘may neither receive nor seek instructions from the Directorate General of Public Finances, nor from any other authority, in the performance of their duties’. Consequently, their functions may only be terminated at the controller’s request or in the event of impediment established, as the case may be, by the vice-president of the Council of State or by the first president or the public prosecutor of the Court of cassation, upon referral by the minister responsible for the budget.

There are no specific rules and remedies protecting the interests of persons concerned by those requests as well as those of the OSPs.

⁵⁰ Article L 96 G II of the Tax Procedures Book.

⁵¹ Article R 96 G-1 of the Tax Procedures Book.

⁵² Article L 96 II of the Tax Procedures Book.

⁵³ According to Article R 96 G-4 of the Tax Procedures Book, the authorisation request and the authorisation itself are ‘made in writing and transmitted by any means that ensures confidentiality and proof of receipt’.

3.1.3. Punitive enforcement in the area of banking law and financial markets

As already explained, in the context of banking and financial law, there are two distinct authorities. Although the ACPR is theoretically competent to sanction both supervised entities and individuals, the issue of accessing telecommunication metadata or any other data collected by OSPs has not arisen for this authority, likely because it has no practical utility. Thus, for this authority, there exists only a general power of inspection. It is with the AMF that the question has arisen, and for this reason, as in most sectors, it is necessary to distinguish between a special power to access telecommunication metadata⁵⁴ and a general power to issue productions order, which can be directed at anyone holding relevant data.

The agents of the AMF can request the same OSPs as for the aforementioned special legal bases, namely electronic communications operators and service providers (see Section 2).

The nature of the data that can be accessed is not defined in that specific law. The reference to Article L. 34-1 of the Post and Electronic Communications Code and Articles 6 I 1 and 2 of Law no. 2004-575 implies that only data subject to data retention obligations are covered (see Section 2).

This legal basis can be used for the purposes of investigating market abuse as defined by Regulation (EU) No. 596/2014 of the European Parliament and of the Council of April 16, 2014 on market abuse (Market Abuse Regulation).

As in other sectors, access to telecommunication metadata was modified following decisions of the Constitutional Council and the ECJ. This procedure is subject to prior authorisation by a controller. Article L 621-10-2 of the Financial and Monetary Code substantiates the authorisation procedure and is very similar to what was already explained regarding the tax administration (see Section 3.1.2). One should only mention that the controller is independent and ‘may neither receive nor seek instructions from the AMF, nor from any other authority, in the performance of his duties’. Consequently, its functions may only be terminated at the controller’s request or in the event of impediment established, as the case may be, by the vice-president of the Council of State or by the first president of the Court of cassation or the public prosecutor at the Court of cassation, upon referral by the Minister for the Economy.

The controller is bound by professional secrecy.⁵⁵

⁵⁴ Article L 621-10-2 of the Monetary and Financial Code.

⁵⁵ Under the conditions set out in Article L 621-4 of the Monetary and Financial Code.

The controller is seized by a reasoned request from the Secretary General or Deputy Secretary General of the AMF, which must include all information required to justify its use. The request for authorisation to disclose telecommunication metadata shall specify for each investigation: 1° The name of the person suspected of having committed market abuse or the name of any other person for whom access to connection data appears necessary for the investigation or, where applicable, the telephone number, IP address or any other metadata data in the possession of the investigators and for which additional elements are necessary for the investigation; 2° The metadata data or types of metadata data requested for each person or in each case mentioned in 1°; 3° The periods for which connection data is requested; 4° The factual and legal grounds for the request.⁵⁶ The authorisation is added to the investigation file.⁵⁷

The request for an authorisation and the authorisation itself ‘shall be made in writing and sent by any means that ensures confidentiality and proof of receipt’.⁵⁸

Article L 621-10-2 of the Monetary and Financial Code contains elements regarding data processing that are likely meant to minimise (in a way) data processing operations, thus protecting the interests of the persons. Firstly, the investigators are allowed to use the data communicated by OSPs exclusively for the purposes of the investigation for which they have received authorisation. Secondly, data relating to facts which are the subject of a notification of grievance by the AMF Board are destroyed six months after the final decision of the Enforcement Committee or the appeal courts.⁵⁹ In the absence of a notification of grievances by the AMF Board, they are destroyed one month after the Board’s decision. Thirdly, in the event of transmission of the investigation report to the Financial Public Prosecutor or in the event of initiation of public proceedings by the Financial Public Prosecutor, the telecommunication data shall be remitted to the Financial Public Prosecutor and shall not be retained by the AMF. The requests for authorisation to access data addressed to the controller as well as the authorisation issued by them should be destroyed in the same condition.⁶⁰ At the end of the retention period, the destruction of the data ‘shall give rise to a report drawn up by

⁵⁶ Article R 621-35-1 I of the Monetary and Financial Code.

⁵⁷ If necessary, additional requests may be submitted in respect of an investigation for which a request has already been made.

⁵⁸ Article R 621-35-1 II of the Monetary and Financial Code.

⁵⁹ The purpose of this is to inform the concerned persons that, after a control of the AMF, punitive administrative proceedings will be open.

⁶⁰ Article R 621-35-3 of the Monetary and Financial Code.

AMF investigators’.⁶¹ The data should be stored, until it is destroyed, in accordance with procedures designed to guarantee confidentiality.⁶²

There is no specific basis to sanction OSPs in case of non-cooperation. It seems that the general power to sanction the absence of cooperation with the AMF can be used in this context.⁶³ The sanction is ‘financial penalty not exceeding 100 million euros or ten times the amount of the benefit gained from the violation, if such benefit can be determined’.⁶⁴

There are no specific remedies available to the persons concerned by the measure or the OSPs.

3.1.4. Competition law enforcement

The legal framework applicable to the access of data held by OSPs by the competition law authority is, like most other sectors, divided into several subcategories of administrative investigative measures. The first specific subcategory concerns access to telecommunication metadata held by certain OSPs. This power was not, however, separated from a general production power,⁶⁵ but is still distinct from the traditional power of search and seizure, which can be used to access other categories of data (see Section 3.2.4).

Article L 450-3-3 of the Commercial Code regulates data processed by electronic communications operators, under the conditions and within the limits provided for in Article L 34-1 of the Post and Electronic Communications Code, and the service providers mentioned in 1 and 2 of I of Article 6 of Law no. 2004-575 (see Section 2). Regarding the type of data that may be requested, the legal basis mentions ‘data stored and processed’ by the aforementioned OSPs. Access can be requested ‘for the purposes of investigating and establishing the offences and breaches provided for in title II of book IV of the Commercial Code’, which is the basis of all the offences related to competition law, such as anti-competitive agreements and practices.⁶⁶

An administrative act, codified in Article R 450-4 to -8 of the Commercial Code, defines the rules of transfer of data.⁶⁷ According to Article

⁶¹ Article R 621-35-3 of the Monetary and Financial Code.

⁶² Article R 621-35-2 of the Monetary and Financial Code.

⁶³ Article L 621-15 II f) of the Monetary and Financial Code.

⁶⁴ Article L 621-15 III c) of the Monetary and Financial Code.

⁶⁵ The Constitutional Council stroke down a reform, before it entered into forced, extending Article L450-3 of the Commercial Code to allow access to metadata. See Conseil Constitutionnel, 05.08.2015, no. 2015-715 DC, § 134-138.

⁶⁶ Article L420-1 of the Commercial Code.

⁶⁷ Decree no. 2019-1247 of 28.11.2024 regarding the procedure for the communication of connection data to the officers mentioned in Article L. 450-1 of the Commercial Code (*Décret*

R 540-4 of the Commercial Code the request for authorisation to disclose telecommunication metadata shall specify for each investigation: ‘1° The name of the person suspected of having taken part in the offences (...) or the name of any other person for whom access to connection data appears necessary for the investigation or, where applicable, the telephone number, IP address or any other connection data in the possession of the investigators and for which additional elements are necessary for the investigation; 2° The connection data or types of connection data requested for each person or in each case mentioned in 1°; 3° The periods for which connection data is requested; 4° The factual and legal grounds for the request’.

As for the other legal bases related to telecommunication metadata access, the main specificity concerns the authorisation of the request.⁶⁸ This procedure ‘is subject to a request for prior authorisation from the general rapporteur of the Competition Authority or the administrative authority in charge of competition and consumer affairs⁶⁹ to a controller of requests for telecommunication data’.

Just like for the other legal provisions where this controller is mentioned, this authority is composed of two persons, namely the controller and their deputy and follow the same rules as in the provisions under the area of banking law and financial markets (see Section 3.1.3).

The request for authorisation shall indicate the elements gathered by the agents mentioned in Article L 450-1 of the Commercial Code, giving rise to a presumption of the existence of an infringement or breach mentioned in title II of the Code, and justifying access to telecommunication data for the purposes of the investigation. Furthermore, the authorisation ‘shall be made in writing and transmitted by any means that ensures confidentiality and attests to receipt’.⁷⁰

Article 450-3-3 II of the Commercial Code protects the interests of the persons concerned by the requests. The metadata shall be used exclusively in the context of the investigation for which the agents have received authorisation to access it. The authorisation order itself is added to the investigation file. Moreover, ‘the data is destroyed six months after a final

relatif à la procédure de communication des données de connexion aux agents mentionnés à l'article L. 450-1 du code de commerce).

⁶⁸ Article L 450-3-3 II of the Commercial Code.

⁶⁹ This authority includes : ‘1° The Director General of Competition, Consumer Affairs and Fraud Control or his appointed representative; 2° The Head of the National Investigations Department of the Directorate General for Competition, Consumer Affairs and Fraud Control or his appointed representative; 3° The Regional Director for Business, Competition, Consumer Affairs, Labour and Employment or his appointed representative; 4° The Director of Enterprise, Competition, Consumer Affairs, Labour and Employment or his appointed representative’, Article R 450-8 of the Commercial Code.

⁷⁰ Article R 450-4 II of the Commercial Code.

decision by the Competition Authority, the administrative authority responsible for competition and consumer affairs, or a judicial or administrative court'. The data relating to facts not subject to prosecution are destroyed one month after the decision of the general rapporteur of the Competition Authority or the competent administrative authority or the judicial or administrative jurisdiction, without prejudice to their transmission to the public prosecutor in application of Article 40 of the Code of Criminal Procedure in case of suspicion of a criminal offence.

Moreover, the data transmitted 'is collected and kept, until it is destroyed, in accordance with procedures designed to guarantee its confidentiality'.⁷¹ The destruction of this data 'gives rise to a report drawn up by the officers mentioned in Article L 450-1'.⁷² Similarly, 'requests for authorisation to access connection data sent to the controller of connection data requests and authorisations issued by the latter are destroyed under the same conditions'.⁷³

There are seemingly no specific rules regarding the sanctions in case of non-cooperation. Article L 450-9 of the Commercial Code applies to any refusal to cooperate in an administrative cooperation undertaken by the Competition Authority: 'It is an offence punishable by two years of imprisonment and a fine of 300.000 euros for any natural person to oppose the performance of the duties entrusted to the agents mentioned in I of Article L 450-1 pursuant to this book'.

3.1.5. GDPR enforcement

Article 19 of the French Data Protection Act provides for a legal basis regarding both production orders as well as visits (see Section 3.2.5). However, none of these provisions directly target OSPs or any type of specific private actor.

3.2. General production orders and search and seizure powers

3.2.1. Customs enforcement

As explained, access to telecommunication metadata used to be grounded on the general legal basis allowing Customs to access different types of data.⁷⁴ This general basis was struck down by the Constitutional Council insofar as access to telecommunication metadata was concerned, which is why there is now a special power entrusted to customs authorities to

⁷¹ Article R 450-5 of the Commercial Code.

⁷² Article R 450-6 of the Commercial Code.

⁷³ Article R 450-6 of the Commercial Code.

⁷⁴ Article 65 of the Customs Code.

access this information.⁷⁵ In spite of this, the general power still exists and is used to access any other kind of data. As a matter of facts, although this general legal basis provides a power to ‘see papers and data’, it also contains a general basis to compel cooperation from ‘all natural or legal persons directly or indirectly involved in regular or irregular operations falling within the remit of the Customs department’.⁷⁶ Notably, in the context of customs, there are also different special legal provisions, one of them dealing, for example, with access to data relating to unidentified persons, which will not be studied here.⁷⁷

The general power of Customs covers ‘papers and documents of any kind relating to operations of interest to their department, whatever their medium’. In other words, except the data covered by the special text (see Section 3.1.1), this general text covers any type of data.

Access is entrusted to ‘customs officers with at least the rank of controller’, on the condition that it is related to ‘of interest to their department’.⁷⁸ The weakness of this control mechanism is the reason why the Constitutional Council did not accept that it could be used to access sensitive data such as telecommunication metadata.

Rules regarding transfer of data are not further defined. Article 65 of the Customs Code only states that ‘The production order is exercised on the spot or by correspondence, including electronically, and regardless of the medium used to store the documents’.

Any refusal to provide the information or documents requested is punishable by a fine of 3.700 euros.⁷⁹ Moreover, ‘offenders must be ordered to produce the books, records or documents that have not been disclosed, subject to a penalty of at least 150 euros for each day’s delay’.⁸⁰ There are no specific rules protecting the interests of persons concerned by those requests, and no remedies available to the addressees of the requests.

3.2.2. Tax enforcement as regards VAT

Article L 16B of the Tax Procedures Book is a general power of the tax administration for investigations related to tax law, including but not limited

⁷⁵ See former Article 65 1° i) of the Customs Code. Conseil constitutionnel, 15.02.2019, 2018-764 QPC, § 8.

⁷⁶ Article 65 1° j) of the Customs Code.

⁷⁷ Article 65 bis A Customs Code. On this, see Decree no. 2024-267 of 26.03.2024 establishing the conditions for exercising the right of communication mentioned in Article 65 bis A of the Customs Code (*Décret fixant les conditions d'exercice du droit de communication mentionné à l'article 65 bis A du code des douanes*).

⁷⁸ Article 65 of the Customs Code.

⁷⁹ Article 413 bis 2° of the Customs Code.

⁸⁰ Article 431 of the Customs Code.

to VAT.⁸¹ It allows ‘conducting visits to any locations, including private ones, where the related documents and records may be held, accessed, or available, and to seize them, regardless of their format’.⁸² During such a visit, information from occupants of the premises or their representative may also be sought.⁸³ The specific case of access to documents on an electronic medium is taken into consideration, although no reference is made to OSPs.⁸⁴

This power can be conducted whenever there are presumptions that a taxpayer does not respect the law, and in particular presumptions that the taxpayer is ‘making purchases or sales without invoices, using or issuing invoices or documents that do not relate to actual transactions’. The visit cannot take place during the night and, further conditions apply in case of absence of the occupant.⁸⁵

The visit can take place only under the authority of an agent of at least the rank of inspector and empowered by the Director General of Public Finances. Furthermore, this visit must be authorised by an order of the judge of freedoms and detention.⁸⁶

The occupant is notified of the visit and can challenge the order allowing it, since it can be appealed before the first president of the court of appeal in the jurisdiction where the judge authorised the measure, within at time limit of fifteen days in principle, and then challenged before the Court of Cassation, still withing a time limit of fifteen days.⁸⁷ After the visit, a report

⁸¹ One could also mention Article L10 of the Tax Procedures Book, according to which the tax administration has the general power to ‘request from taxpayers any information, justifications, or clarifications relating to the filed declarations or submitted documents’. In theory, this provision could allow the administration to request information from third parties in an administrative investigation, provided that these third parties are also taxpayers. However, there are no precise rules confirming or refuting such an interpretation. It should be noted that this power to ‘request’ is not binding. In other words, refusing to provide the requested information will not be sanctioned, as the administration has other coercive means to access the information. One could thus imagine this article being used to seek the voluntary cooperation of service providers. Nevertheless, it is worth noting that Article L10 of the Tax Procedures Code Books also refers to a ‘charter of rights and obligations of the audited taxpayer’. This suggests that the article is intended to govern only the relationship between the administration and the audited taxpayer.

⁸² Article L 16B I of the Tax Procedures Book.

⁸³ Article L 16B III bis of the Tax Procedures Book.

⁸⁴ Article L 16B VI bis of the Tax Procedures Book. This legal basis addresses cases of obstruction but also the procedures of seizing such mediums and the defense rights of the concerned persons.

⁸⁵ Article L 16B III of the Tax Procedures Book. This legal basis limits the number of persons allowed to review the documents and ensures compliance with professional secrecy and the rights of the defense.

⁸⁶ Article L 16B II of the Tax Procedures Book clarifies the role of the judge.

⁸⁷ Article L 16B II of the Tax Procedures Book clarifies the role of the judge.

is drafted, notably to make an inventory of the seized document,⁸⁸ and this information is given to the occupant as well as to the presumed offender justifying the visit.⁸⁹

3.2.3. Punitive enforcement in the area of banking law and financial markets

A general basis was previously used to access telecommunication metadata before the intervention of the Constitutional Council.⁹⁰ The legal basis covers ‘any person’ and allows access to ‘any documents, regardless of their medium’. Investigators and inspectors are allowed to request data ‘for the purposes of the investigation or inspection’. It seems that no administrative act detailing these conditions was published. In case of non-cooperation, the same sanctions as those attached to the special provision to obtain telecommunication metadata are applicable (see Section 3.1.3).⁹¹ There are no specific rules related to authorisation or control, nor protecting the interests of persons concerned by those measures.

3.2.4. Competition law enforcement

There are two general provisions which can be seen as general bases for the competition authority to obtain data. The applicable provision will depend on the type of premises the agents are willing to search.

Article L 450-3 of the Commercial Code does refer to third party specifically, although it targets premises used for business purposes. According to this provision, the agents may operate in ‘any premises used for business purposes or where services are being provided, and gain access to any means of transport used for business purposes’. They can also access these premises when they are also (and therefore not only) used for residential purposes. The agents ‘may demand to see, obtain or take copies, by any means and on any medium, of books, invoices and other business documents of any kind, and, where applicable, of their means of deciphering, likely to be held or to be accessible or available, wherever they may be, to facilitate the performance of their duties’.⁹² Although OSPs are not mentioned, the specific situation of control of ‘computerised operations’ is mentioned, seemingly referring to any kind of stored data. In such case, the agents ‘have access to

⁸⁸Article L 16B IV of the Tax Procedures Book.

⁸⁹Article L 16B V of the Tax Procedures Book.

⁹⁰Article L 621-10 of the Monetary and Financial Code.

⁹¹Article L 621-15 II f) of the Monetary and Financial Code.

⁹²They may demand that they be provided with the resources they need to carry out their checks. They may also obtain, on the spot or when summoned, any information, document or justification required for the audit.

software and stored data, as well as to the unencrypted reproduction of information likely to facilitate the accomplishment of their missions. They may request the transcription of documents directly usable for control purposes, using any appropriate processing method'.⁹³ In principle, these visits are allowed only between 8 a.m. and 8 p.m. Premises used for business purposes can however be entered 'outside these hours if they are open to the public, or if production, manufacturing, processing, packaging, transport or marketing activities are underway [...] with judicial authorisation given by order of the judge of freedoms and detention of the judicial tribunal within the jurisdiction where the places to be visited are located'.

The second procedure, based on Article L 450-4 of the Commercial Code, is broader in scope but more strictly regulated. It provides for 'visits to all locations, as well as the seizure of documents and any information medium'. The conditions regarding the time of the visit are stricter since it 'cannot begin before 6 a.m. or after 9 p.m., [and should be] conducted in the presence of the occupant of the premises or their representative'. Such measures must be part of 'investigations requested by the European Commission, the Minister in charge of the economy, or the General Rapporteur of the Competition Authority upon the recommendation of the Rapporteur, with judicial authorisation given by order of the judge of freedoms and detention of the judicial tribunal within the jurisdiction where the places to be visited are located'.⁹⁴ The task of the judge is to verify that 'the request for authorisation submitted to them is justified; this request must include all the information in the applicant's possession that justifies the visit'.⁹⁵ This judge is also entrusted with the supervision of the visit and seizure.⁹⁶ The occupant of the premises or their representatives are verbally notified, informed of their rights and receive a full copy of the order.⁹⁷ The order rejecting the request for an authorisation can be appealed to the first president of the court of appeal in the jurisdiction where the judge authorised them, following the rules provided by the Code of Criminal Procedure by the Competition authority of the Minister of the Economy.⁹⁸ The authorisation can be appealed, by the public prosecutor or the person against whom the order was issued.⁹⁹ Once the authorisation is granted, the occupant 'may

⁹³ Article L 450-3 § 5 of the Commercial Code.

⁹⁴ Article L 450-4 of the Commercial Code.

⁹⁵ When the visit is aimed at identifying infractions to the provisions of Book IV of this Code that are in progress, the authorisation request may include only the indications necessary to presume the existence of the practices being investigated.

⁹⁶ 'The judge may visit the premises during the intervention. At any time, they may decide to suspend or terminate the visit'. Article L 450-4 § 4 of the Commercial Code.

⁹⁷ Article L 450-4 § 5 of the Commercial Code.

⁹⁸ Article L 450-4 § 6 of the Commercial Code.

⁹⁹ Article L 450-4 § 6 of the Commercial Code.

designate one or more representatives to attend the visit and sign the report'. If this is impossible, for example because the occupant is not present, 'the judicial police officer summons two witnesses chosen from outside those under their authority, that of the General Directorate for Competition, Consumer Affairs and Fraud Control, or the Competition Authority'. The list of persons allowed to inspect the document before the seizure is strictly limited.¹⁰⁰ During the visit, the agents can conduct interviews.¹⁰¹ After the visit, 'Inventories and sealing of items are carried out' following the conditions applicable to search and seizure in criminal procedure,¹⁰² moreover 'the original of the report and the inventory are submitted to the judge who ordered the visit', 'a copy of the report and the inventory is provided to the occupant of the premises or their representative' and 'a copy is also sent by registered letter with acknowledgment of receipt to individuals later implicated by the items seized during the operation'.

Seized documents and items must be 'returned to the occupant of the premises within six months from the date the decision of the Competition Authority becomes final'.¹⁰³ In such case, 'the occupant is notified by registered letter with acknowledgment of receipt to retrieve the items within two months'.¹⁰⁴ The conduct of the visit and seizure operations may be challenged in an appeal to the first president of the court of appeal in the jurisdiction where the judge authorised them, following the rules provided by the Code of Criminal Procedure, by the public prosecutor or the person against whom the order was issued, or the individuals implicated by the items seized during these operations, within ten days after they received notification of the procedure, and then challenged before the Court of cassation.¹⁰⁵ Pending a final decision, the seized items are kept in the aforementioned conditions.¹⁰⁶

¹⁰⁰ Article L 450-4 § 8 of the Commercial Code. The agents mentioned in Article L. 450-1, the occupant of the premises or their representative, as well as the judicial police officer and, where applicable, agents and other persons mandated by the European Commission, are the only ones authorised to inspect the documents before their seizure.

¹⁰¹ Article L 450-4 § 8 of the Commercial Code. During the interviews, specific rules apply in case of suspicion of a criminal offence: 'In accordance with Article 28 of the Code of Criminal Procedure, Article 61-1 of the same Code applies when a person is interviewed, and there are reasonable grounds to suspect that they have committed or attempted to commit an offence'.

¹⁰² In accordance with Article 56 of the Code of Criminal Procedure. Article L 450-4 § 9 of the Commercial Code.

¹⁰³ Article L 450-4 § 10 of the Commercial Code.

¹⁰⁴ Article L 450-4 § 11 of the Commercial Code. If the occupant fails to act by this deadline, the items and documents are returned at their own expense.

¹⁰⁵ Article L 450-4 § 12 of the Commercial Code.

¹⁰⁶ Article L 450-4 § 12 of the Commercial Code.

As far as the sanction is concerned, ‘anyone who opposes the exercise of the functions of agents of the Competition Authority is punishable by two years of imprisonment and a fine of 300.000 euros’.¹⁰⁷

3.2.5. GDPR enforcement

Based on Article 19 I of the Data Protection Act, the ‘members of the Data Protection Authority and the agents of its departments’ are authorised to take part in visits according to article 10 have access ‘from 6 a.m. to 9 p.m., for the performance of their duties, to places, premises, enclosures, installations or establishments used for the implementation of personal data processing’. The public prosecutor is informed of their actions. A specific authorisation is necessary ‘when personal data processing is implemented, either in the parts of these places, premises, enclosures, installations or establishments allocated to private purposes, or in such places, premises, enclosures, installations or establishments entirely allocated to private purposes’. In such case, ‘the visit may only take place after authorisation from the judge of freedoms and detention of the judicial court in whose jurisdiction the premises to be visited are located’.¹⁰⁸ Moreover, based on Article 19 II of the Data Protection Act, the person in charge of the ‘places, premises, enclosures, installations or establishments’ that are visited ‘is informed of their right to object to the visit’. In case of an objection, ‘the visit may only take place after authorisation from the liberty and custody judge of the judicial court in whose jurisdiction the premises to be visited are located’.¹⁰⁹ Where justified by the urgency or seriousness of the facts giving rise to the inspection, or by the risk of documents being destroyed or concealed, the visit may take place without informing the person in charge of the premises, so that this person cannot object and trigger the necessity to get an authorisation from the judge of freedoms and detention.¹¹⁰ This procedure requires continuous supervision by the judge of freedoms and detention.¹¹¹ The authorisation may be appealed, in accordance with the rules laid down in the Code of Civil Procedure, to the first president of the court of appeal.¹¹²

The agents of the Authority are also entrusted with further powers based on Article 19 III of the Data Protection Act.¹¹³ They ‘may request

¹⁰⁷ Article L450-8 of the Commercial Code.

¹⁰⁸ Article 19 I § 3 of the Data Protection Act

¹⁰⁹ Article 19 II of the Data Protection Act

¹¹⁰ Article 19 II § 1 of the Data Protection Act

¹¹¹ Article 19 II § 2 of the Data Protection Act

¹¹² Article 19 II § 3 of the Data Protection Act

¹¹³ On the top of the requests they may make, this article also covers the observations that they can add based on the use of online public communications services: ‘In addition to

communication of all documents necessary for the performance of their tasks, regardless of the medium, and take copies thereof'. They may obtain, on site or when summoned, any information and justification useful and necessary to the performance of their duties. They may access computer programs and data, under conditions that maintain confidentiality with respect to third parties, and request that they be transcribed by any appropriate process into documents that can be used directly for the purposes of the audit. The scope of the data they can access is therefore very broad. Notably, 'Secrecy may not be invoked against them, except in the case of information covered by professional secrecy applicable to relations between a lawyer and their client, by the secrecy of journalistic sources or [...] medical secrecy'.¹¹⁴

3.3. Requests to online service providers: the bigger picture

To understand the issues of administrative access to data held by OSPs, it is essential to put this legal framework into perspective with the frameworks applicable to criminal procedure and intelligence gathering.

In these contexts, the evolution of the framework governing access to data held by OSPs has been much more complex and controversial than in the administrative context. Indeed, the Council of State refused to align its position with the case law of the ECJ following the *La Quadrature du Net*

carrying out on-site inspections and when summoned, they may make any useful observations. In particular, they may use online public communication services to consult data that is freely accessible or has been made accessible, including through carelessness, negligence or the act of a third party, where necessary by accessing and remaining in automated data processing systems for the time required to make their observations. They may transcribe data by any appropriate means into documents that can be used directly for the purposes of the inspection.

For the control of online public communication services, the members and agents mentioned in the first paragraph of I may carry out any online operation necessary for their mission under an assumed identity. Under penalty of nullity, their actions may not constitute incitement to commit an offence. The use of an assumed identity has no effect on the legality of the findings made in accordance with the third paragraph of this provision III. A decree issued after consultation with the Council of State, issued after consultation with the CNIL, specifies the conditions under which such members and agents shall make their findings in such cases. The members and agents mentioned in the first paragraph of provision I may, at the request of the Commission Chairman, be assisted by experts. Minutes are drawn up of verifications and visits carried out in application of the present article. Such minutes shall be drawn up in the presence of both parties when the verifications and visits are carried out on site or when summoned'.

¹¹⁴ Medical secrecy applies to information contained in data processing for the purposes of preventive medicine, medical research, medical diagnosis, the administration of care or treatment, or the management of health services. Individual medical data included in this category of processing may only be communicated under the authority and in the presence of a doctor.

I ruling.¹¹⁵ Subsequently, the Constitutional Council and the legislature adopted very minimalist approaches, refusing to consider that French law should evolve significantly in this area.¹¹⁶ It was ultimately the Court of Cassation that ruled that the criminal procedures regulating access to the telecommunication metadata, namely production orders (*réquisitions*), had to be aligned with the case law of the ECJ, thus requiring that such orders could no longer be authorised solely by a public prosecutor and must be limited to investigations of serious crimes.¹¹⁷ The Constitutional Council was not at all at the origin of the shift towards a better integration of the principles put forward by the ECJ. From this perspective, it is clear that the aforementioned evolution of the legal framework triggered by Constitutional Council in the very specific case of access to telecommunication metadata in the administrative framework was a minor concession to European requirements rather than evidence of a genuine desire to modernise French legislation.

Furthermore, metadata are not the only types of data held by OSPs that may be of interest in the context of an investigation. Whether in the administrative or criminal domain, there has been no significant transformation of the French legal framework to strictly regulate or adapt it to the realities of cooperation between the public sector and private actors, who may be located abroad. Although this debate does not even exist in the context of administrative investigations, legal scholars regularly criticise the lack of proper regulation concerning the tools available to investigators for conducting digital searches in criminal investigations. Yet these instruments can be considered far more intrusive than access to telecommunication metadata.¹¹⁸

Last but not least, the issue of notification to the data subject or the affected person after access was undertaken, is almost entirely absent from the scholarship, both in criminal procedure and in the administrative context. In other words, the unavailability of separate remedies from those that exist when data is used as evidence, is not even a discussion. In all the aforementioned decisions of the Constitutional Council, the Council ruled

¹¹⁵ ECJ, *La Quadrature du Net I*, 06.10.2020, C-511/18. See, M. Lassalle, 'Protection des données, renseignement, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE', *Recueil Dalloz*, 2021, p. 406.

¹¹⁶ Conseil d'Etat, *French Data Network*, 21.04.2021, 393099; Conseil constitutionnel, 03.12.2021, 2021-952 QPC; Conseil constitutionnel, 20.05.2022, 2022-993 QPC; Conseil constitutionnel, 17.06.2022, 2022-1000 QPC. See M. Lassalle, 'Conservation et réquisition des données relatives aux communications électroniques : un débat serein est-il enfin possible ?', *Recueil Dalloz*, 2022, p. 1540.

¹¹⁷ Cour de cassation, Chambre criminelle, 12.06.2022, 21-83.710.

¹¹⁸ S. Sontag-Koenig, 'La transformation des actes d'enquête : de la perquisition (informatique) aux autres techniques de captation', *Actualité Juridique Pénal*, 2023, p. 486; S. Sontag Koenig, 'Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel', *Actualité Juridique Pénal*, 2016, p. 238.

only once on the right of notification of the affected person and the right to appeal a data request in the context of administrative investigations.¹¹⁹ Based on such ruling, access as such does not require a notification to the data subject nor the right to challenge the measure. Investigative acts interfering with the right to privacy do not give ground to a remedy. The principle is that their legality can only be challenged once the information derived from these measures is used as evidence.¹²⁰ Although this approach is debatable, it is very much in line with the French conception of an effective remedy that also applies in the context of criminal investigations.¹²¹ The basic idea is that judicial supervision, access to remedies once the data is used as evidence, and the possibility to sue the state in case of serious misconduct, is deemed sufficient to consider that concerned persons have access to an effective remedy.

4. TRANSFER OF DATA BETWEEN PROCEEDINGS

The transfer of evidence between proceedings has not, in itself, been the subject of significant legislative development—the regulation of evidence itself is not unified—nor has it been extensively addressed in the legal literature.¹²² The even more specific question of rules governing the transfer of a specific category of evidence, namely information obtained from OSPs, is even less present. However, this section aims to outline the main legal provisions used for such transfers, at least to identify the questions that have attracted the attention of the legislature.

4.1. Transfers of data between national proceedings

Regarding the transfer of data from one administrative procedure to another or to criminal proceedings, there are no general rules, and there are certainly no specific rules concerning evidence obtained through cooperation with OSPs. However, there is a particular risk highlighted by legal scholars regarding the transfer of data between different procedural frameworks: the circumvention of the safeguards specific to criminal procedure through the use of investigative measures in an administrative context. Actions taken in an administrative context are generally considered to be subject to less strict

¹¹⁹ Conseil Constitutionnel, 14.06.2019, 2019-789 QPC.

¹²⁰ For a criticism of such a conception, in the specific context of administrative cooperation in tax matters, see ECJ, *Opinion of Advocate General Kokott*, 02.07.2020, C-245/19 and C-246/19.

¹²¹ Lassalle, (n. 32).

¹²² Matsopoulou, (n. 10), pp. 163-176.

regulation and, therefore, are potential tools to circumvent the guarantees in criminal procedure.¹²³

Yet, sectorial legislations barely regulate transfers of data between national proceedings. The Customs Code specifies that public authorities may not invoke professional secrecy against requests made by customs officers with at least the rank of controller for access to documents held by these authorities.¹²⁴ The same goes for requests from the tax administration.¹²⁵ Furthermore, the law authorises spontaneous and on request cooperation among the tax administration, the Customs administration and agents in charge of competition law.¹²⁶ Similarly, the AMF, the ACPR, and other administrative authorities (notably in matters of competition and customs) can freely exchange data.¹²⁷ As far as the Competition Authority is concerned, its agents ‘may, without being subject to the obligation of professional secrecy, have access to any document or item of information held by State services and establishments’.¹²⁸

As for the transfer of data from criminal proceedings to an administrative procedure, there is also no general rule or any specific rules concerning data collected through OSPs. However, there are, albeit not systematically, sector-specific rules. For example, the public prosecutor can freely disclose information to the tax administration, and the tax administration will have to provide feedback about the subsequent proceedings.¹²⁹

Similarly, any document from criminal proceedings directly related to facts submitted to the Sanctions Commission of the AMF may be communicated by the public prosecutor, either on their own initiative or upon request.¹³⁰ However, nothing on that regard seems to be provided in other sectors.

The general approach regarding the transfer of data from an administrative procedure to a criminal one is provided in Article 40 § 2 of the Code of Criminal Procedure, which states that ‘any constituted authority, public officer, or civil servant who, in the exercise of their duties, becomes aware of a crime or an offence, is required to promptly inform the public prosecutor and to forward to this magistrate all relevant information, reports, and documents’. Despite this, there are also specific provisions. While there

¹²³ Ibid, p. 164.

¹²⁴ Article 64 A of the Customs Code

¹²⁵ Article L 83 of the Tax Procedures Book.

¹²⁶ Article L 83A of the Tax Procedures Book.

¹²⁷ Article L 631-1 of the Monetary and Financial Code.

¹²⁸ Article L 450-7 of the Commercial Code.

¹²⁹ Article L 82C of the Tax Procedures Book. See also Article L 101 of the Tax Procedures Book.

¹³⁰ Article L 621-20-4 of the Monetary and Financial Code.

are no provisions concerning Customs, the tax administration, the Competition Authority, or the CNIL, there are specific provisions regarding the AMF. A first provision reiterates the general rule of the Code of Criminal Procedure.¹³¹ A second provision adds that the public prosecutor may obtain from the AMF all information held by it in the exercise of its duties, without being hindered by professional secrecy.¹³² This latter transmission can be limited, based on Article L 632-16 § 3 of the Monetary and Financial Code, where the data was obtained from a foreign authority.

4.2. Transfers of data between foreign and national proceedings

Only sectorial regulations provide for instances of international cooperation between administrations of the same nature. The tax administration may cooperate with foreign tax administrations based on administrative cooperation in tax matters.¹³³ The ACPR and the AMF may exchange information with European authorities and those of other EU Member States that perform similar functions.¹³⁴ These two authorities may also carry out investigation requests from authorities of other Member States ‘as part of a monitoring activity, an on-site inspection, or an investigation’.¹³⁵ The information received by these two authorities is covered by professional secrecy and is intended solely for the fulfilment of their missions.¹³⁶ The Competition Authority may share information and documents in its possession, or information and documents that it will collect upon request, with the European Commission and authorities of other Member States within the scope of its competencies, subject to reciprocity. In such cases, it must inform the Minister in charge of the economy, and this can only be done ‘on the condition that the foreign authority is subject to professional secrecy with the same guarantees as in France’.¹³⁷ Regarding data protection, the Data Protection Act establishes the principle of intra-

¹³¹ Article L 621-20-1 of the Monetary and Financial Code.

¹³² Article L 621-20-1 of the Monetary and Financial Code.

¹³³ Article L 45 of the Tax Procedures Code.

¹³⁴ Article L 632-1 of the Monetary and Financial Code.

¹³⁵ Article L 632-2 of the Monetary and Financial Code. In both cases, they may “refuse to comply with such a request only when the request is likely to harm French sovereignty, security, or public order, or when a criminal procedure has already been initiated in France based on the same facts and against the same individuals, or if those individuals have already been sanctioned by a final judgment for the same facts”, Article L632-5 of the Monetary and Financial Code.

¹³⁶ Article L 632-3 of the Monetary and Financial Code.

¹³⁷ Article L 462-9 of the Monetary and Financial Code.

European¹³⁸ and extra-European cooperation regarding access to data that is deemed necessary.¹³⁹

There are no specific provisions regarding the cross-procedural transfer of data obtained from a foreign criminal procedure intended for an administrative proceeding in France. The same applies to data originating from a foreign administrative procedure and being incorporated into a criminal procedure in France.

4.3. Admissibility of data collected from online service providers as evidence

The principle in administrative litigation is the freedom of evidence. In other words, once a piece of information is deemed admissible, it will be considered in the judge's analysis. The key issue, therefore, is to determine to what extent information obtained from requests to OSPs can be considered inadmissible as evidence. However, for most of the relevant litigation (AMF, ACPR, Competition Authority), and more generally in administrative litigation, the scrutiny of how authorities have accessed information has historically been very limited.¹⁴⁰

It is worth noting that the issue of the admissibility of data collected from telecommunications operators in the context of an investigation initiated by the AMF—and later transferred to a criminal procedure—has already been the subject of a preliminary ruling. However, the ECJ declined to rule on the procedural rules concerning the admissibility of such data.¹⁴¹

One could argue here that what is lacking is not so much the existence of specific rules regarding the admissibility of evidence, but rather the existence of specific rules concerning access to the evidence (with the understanding that not all information obtained will necessarily be used as evidence). Although the necessity to get an authorisation from an independent authority to use intrusive measures was implemented in the context of administrative investigations, it is still contested in the context of criminal proceedings since the authorisation by the public prosecutor is still deemed, in that context, sufficiently protective. On the top of that, neither criminal procedure nor administrative proceedings open remedies to concerned persons or OSPs in case of productions order. These measures can only be challenged if and once the information derived from the measure is used as

¹³⁸ Article 26 of the Data Protection Act.

¹³⁹ Article 29 of the Data Protection Act.

¹⁴⁰ N. Ida, *La preuve devant l'autorité des marchés financiers*, Paris, Dalloz, 2022, p. 346. There are however sectorial rules related to the admissibility of data originating from abroad, see for instance Ibid. p. 390.

¹⁴¹ ECJ, *Criminal proceedings against VD and SR*, 20.09.2022, C-339/20 and C-397/20.

evidence, which will not necessarily be the case. As a consequence, what is missing is an autonomous remedy to challenge these measures when they are not followed by punitive administrative procedures and therefore used as evidence.

5. CONCLUSION

The current French legal framework highlights two significant trends. Firstly, the specificity of the legal framework related to access to telecommunication metadata—which is relatively recent—should be underscored in comparison to the legal framework applicable to other administrative investigative measures. Secondly, this trend in the context of administrative investigations should be compared to the distinct development within criminal procedure.

Regarding the first trend, while the legal framework has been significantly modified to adapt to the specificities of cooperation with certain OSPs and to access certain types of data, these modifications have only been very partial. In fact, this modification is exclusively attributable to decisions of the Constitutional Council, which, only in the context of administrative investigations, has chosen to follow, at least partially, the case law of the ECJ. Furthermore, these modifications have overlooked other issues of administrative investigations such as notifications and remedies, simply because these issues have not—yet—been addressed by the ECJ.¹⁴² There is thus a clear contrast between the specific regulation of access to telecommunication metadata and the somewhat inconsistent regulation of access to other types of data.

Regarding the second trend, it is evident that the Constitutional Council—and subsequently the legislature—early on partially followed the case law of the ECJ, while the same case law was completely ignored for years in the context of criminal procedure. The numerous developments concerning the production order for telecommunication metadata in criminal procedure did not affect administrative investigations. Indeed, the Constitutional Council, in the administrative context, quickly accepted the idea that oversight by an independent authority was necessary to authorise access to telecommunication metadata. In contrast, it was much more difficult for the Constitutional Council to admit that oversight by a prosecutor alone was insufficient to authorise order to produce telecommunication metadata in

¹⁴² It is noteworthy that the legal framework applicable to searches and seizures in administrative matters was significantly modified following a decision by the European Court of Human Rights directly targeting France (ECtHR, *Ravon v. France*, 21/02/2008, no. 18497/03). The fact remains that such a decision has not yet addressed the issue of access to data held by OSPs.

the criminal procedure. From this perspective, the legislative enshrinement of a telecommunication metadata controller, competent only for certain types of administrative investigations, is particularly noteworthy. Last but not least, French law is not consistent. Although the controller is competent in the fields of tax, financial and competition administrative punitive law, the public prosecutor remains in charge of authorising access to telecommunication metadata in the field of customs.

ANNEX - TABLE: DURATION OF DATA RETENTION BASED ON THE NATURE OF THE INFORMATION AND ON THE PURPOSE OF DATA RETENTION

	For the purposes of criminal proceedings, the prevention of threats against public security, and the safeguarding of national security	For the purposes of the fight against serious crimes, the prevention of serious threats against public security, and the safeguarding of national security	For reasons relating to the safeguarding of national security, (when a serious threat, present or foreseeable, against the latter, is observed¹⁴³)
Information relating to the civil identity of the user¹⁴⁴	Five years (from the end of the validity of the contract)	Five years (from the end of the validity of the contract)	Five years (from the end of the validity of the contract)
Other information provided by the user when subscribing to a contract or creating an account¹⁴⁵ as well as information relating to payment¹⁴⁶	One year (from the end of the validity of the contract or the closing of the account)	One year (from the end of the validity of the contract or the closing of the account)	One year (from the end of the validity of the contract or the closing of the account)

¹⁴³ Decree no. 2022-1327 of 17.10.2024 ordering the retention, in view of the serious and current threat to national security, of certain categories of connection data for a period of one year (*Décret portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion*).

¹⁴⁴ Article R 10-13 I of the Code of Posts and Electronic Communications. The same goes for the actors covered by Articles 6 I 1 and 2 of Law no. 2004-575. See Article 2 Decree no. 2021-1362 of 20.10.2021 regarding the retention of data enabling the identification of any person who contributed to the creation of content posted online, enacted pursuant to Section II of Article 6 of Law no. 2004-575 (*Décret relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, pris en application du II de l'article 6 de la loi n° 2004-575 pour la confiance dans l'économie numérique*).

¹⁴⁵ Article R 10-13 II of the Code of Posts and Electronic Communications. The same goes for the actors covered by Articles 6 I 1 and 2 of Law no. 2004-575. See Article 3 Decree no. 2021-1362.

¹⁴⁶ Article R 10-13 III of the Code of Posts and Electronic Communications. The same goes for the actors covered by Articles 6 I 1 and 2 of Law no. 2004-575. See Article 4 of Decree no. 2021-1362.

Technical data making it possible to identify the source of the connection or those relating to the terminal equipment used¹⁴⁷	No data retention is allowed.	One year (from the connection or use of the terminal equipment)	One year (from the connection or use of the terminal equipment)
Certain categories of traffic data, in addition to the technical data mentioned above, and location data specified by decree¹⁴⁸	No data retention is allowed.	No data retention is allowed.	Up to one year, under the condition that the Prime Minister requests electronic communications to do it for certain categories of data

Source: M. Lassalle, ‘A Clash Between the French System and the CJEU Case Law on Data Retention?’ in: Eleni Kosta, I. Kamara (eds.), *Data Retention in Europe and beyond: Law and Policy in the aftermath of an invalidated directive*, Oxford, OUP, forthcoming.

¹⁴⁷ Article R 10-13 IV of the Code of Posts and Electronic Communications. Similar obligations apply to the actors covered by Articles 6 I 1 and 2 of Law no. 2004-575. See Article 5 Decree no. 2021-1362.

¹⁴⁸ Article R 10-13 V of Code of Posts and Electronic Communications. Similar obligations apply to the actors covered by Articles 6 I 1 and 2 of Law no. 2004-575. See Article. 6 of Decree no. 2021-1362.

7. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN GERMANY

P. BLUME, M. GAHN, J. REICHMANN, C. ZOLLER, and D. BRODOWSKI

1. COMPETENT AUTHORITIES IN SELECTED AREAS OF PUNITIVE ADMINISTRATIVE ENFORCEMENT¹

1.1. Competent authorities in customs enforcement

The German customs administration is divided into several administrative bodies which are part of the federal revenue authorities.² The Central Customs Authority³ is a higher federal authority managing the execution of the duties and responsibilities of the customs administration and overseeing the main customs offices⁴ and the customs investigation offices.^{5,6} It has eleven directorates, among them the Customs Criminal Office,⁷ the central agency for customs investigations.⁸ The main customs offices are local authorities responsible for the managing of customs,⁹ whereas the customs investigation offices are local authorities in charge of customs investigations.¹⁰

There is no provision that directly stipulates a specific customs authority to be generally competent for punitive administrative proceedings.

¹ Translations of some important German acts can be found on the website of the Federal Ministry of Justice at https://www.gesetze-im-internet.de/Teilliste_translations.html. The terminology used in this text to describe German legal terms is in parts based on these translations.

² § 6 (2) no. 2, 5 Fiscal Code (*Abgabenordnung*, ‘AO’), § 1 Revenue Administration Act (*Finanzverwaltungsgesetz*, ‘FVG’). German national customs laws, as relevant in the scope of this project, are mainly the FVG, the Customs Administration Act (*Zollverwaltungsgesetz*, ‘ZollVG’), and the Customs Investigations Act (*Zollfahndungsdienstgesetz*, ‘ZFdG’).

³ *Generalzolldirektion*.

⁴ *Hauptzollämter*.

⁵ *Zollfahndungsämter*.

⁶ §§ 1, 5a FVG.

⁷ *Zollkriminalamt*.

⁸ § 5a (2) FVG, §§ 1, 2 ZFdG.

⁹ §§ 1, 12 FVG.

¹⁰ § 1 ZFdG.

The ZFdG mentions both the Customs Criminal Office and the customs investigations offices in relation to ‘the prevention and the prosecution of criminal and regulatory offences’, though in the text of the act’s provisions, the focus lies on the prevention.¹¹

1.2. Competent authorities in tax enforcement as regards VAT

Generally, the revenue authorities are competent in the case of tax-related regulatory offences;¹² more specifically, the revenue authority administering the tax concerned.¹³ As an exception, some (but not all) of the specifically VAT-related regulatory offences in the Value Added Tax Act (‘UStG’¹⁴), are within the area of competence of the Federal Central Tax Office (‘BZSt’¹⁵).¹⁶ In Germany, it is a peculiarity of tax law in contrast to other areas of law that the administrative body itself – the revenue authority – is not only competent to investigate tax-related regulatory offences,¹⁷ but also, within certain boundaries,¹⁸ tax-related criminal offences.¹⁹ When the revenue authority investigates tax-related crimes, it benefits from extended competences, as the restrictions imposed on the administrative authorities investigating regulatory offences²⁰ do not apply and certain measures reserved for the prosecution of (certain) criminal offences are available. This does not, however, blur the lines between the areas of criminal and regulatory offences, which remain two separated categories, each with different proceedings.²¹ Whenever the revenue authority investigates regulatory offences, only the rules concerning this area apply, so that there is strictly an

¹¹ For the Customs Criminal Office, see § 4 ZFdG – the title of the provision mentions the prosecution of regulatory offences, but its text does not. Concerning the customs investigation offices, § 5 ZFdG does consider them to have several responsibilities for the prosecution of regulatory offences in the area of customs administration, but not a general competence. Instead, they may collect and evaluate information and notify the Customs Criminal Office and other customs administration authorities about relevant findings, § 5 (2) (1) ZFdG.

¹² § 409 AO in conjunction with §§ 36 (1) sentence 1, 35 (1) of the Act on Regulatory Offences (*Ordnungswidrigkeitengesetz*, ‘OWiG’).

¹³ §§ 409, 387 (1) AO.

¹⁴ *Umsatzsteuergesetz*.

¹⁵ *Bundeszentralamt für Steuern*.

¹⁶ See § 26a (4) UStG.

¹⁷ § 377 AO.

¹⁸ In particular, it requires the absence of a non-tax criminal offence in the same investigation (§ 386 (2) no. 1 AO). Furthermore, the revenue authority’s competence ends in case an arrest warrant is issued against the suspect (§ 386 (3) AO).

¹⁹ §§ 386, 369 AO.

²⁰ § 46 (2)–(6) OWiG.

²¹ Criminal proceedings are governed by the StPO, whereas regulatory offence proceedings are governed by the OWiG. While the OWiG refers to the procedural rules of the StPO, it also specifies deviations from StPO rules, as discussed in more detail below, 2.1.2.

administrative enforcement. Investigations of criminal offences as well as of regulatory ones are mainly carried out by the Customs Investigation Offices²² and those departments of the revenue authorities responsible for tax investigation and their officials; they have the same rights and obligations as the police authorities and officers according to the German Code of Criminal Procedure ('StPO',²³).²⁴

1.3. Competent authorities in punitive enforcement in the area of banking law and financial markets

The Federal Financial Supervisory Authority ('BaFin',²⁵) is the primary German authority competent to investigate regulatory offences in the area of banking and financial markets. In Germany, the banking sector is regulated in the Banking Act ('KWG',²⁶), whereas securities trading is regulated in the Securities Trading Act ('WpHG',²⁷). Both these acts include regulatory offences in case of violation of certain provisions, and in both areas, the BaFin is the competent authority with regard to the prosecution of these offences.²⁸ Additionally, there is the area of stock exchange supervision, governed by the Stock Exchange Act ('BörsG',²⁹), whose enforcement lies within the competence of the authorities of the federal states.^{30,31} This act also contains provisions on regulatory offences in case of certain violations. The competence for their prosecution resides with the respective state governments (specifically the ministries of finance or ministries of economic affairs), as further regulated within these states' laws.³²

²² *Zollfahndungsdienste*.

²³ *Strafprozessordnung*.

²⁴ § 404 sentence 1 AO (in conjunction with § 410 (1) no. 9 AO). A difference between the competences of the Customs Investigation Offices in criminal and regulatory offence proceedings lies in the fact that in the latter, their officials do not enjoy the competences reserved by law for 'investigators of the public prosecutor's office', as § 410 (1) no. 9 AO does not refer to the second half-sentence of § 404 (2) sentence 2 AO. However, they may be appointed as such by the investigating revenue authority: M. Jäger, '§ 410', in: F. Klein (ed.), *Abgabenordnung*, Munich, Germany, C.H. Beck, 17th ed., 2024, § 17.

²⁵ *Bundesanstalt für Finanzdienstleistungsaufsicht*.

²⁶ *Kreditwesengesetz*.

²⁷ *Wertpapierhandelsgesetz*.

²⁸ § 1 (5) no. 2, § 60 KWG in conjunction with § 36 (1) no. 1 OWiG; § 1 (1) no. 8, § 121 WpHG in conjunction with § 36 (1) no. 1 OWiG.

²⁹ *Börsengesetz*.

³⁰ *Bundesländer*.

³¹ § 3 (1) sentence 1 BörsG.

³² § 36 (1) no. 2 lit. b OWiG.

1.4. Competent authorities in competition law enforcement

On the one hand, with regard to formal *administrative proceedings* – pursuant to § 48 (1) of the Competition Act (‘GWB’³³) – the Federal Cartel Office,³⁴ the Federal Ministry for Economic Affairs and Energy³⁵ and the Supreme State Authorities³⁶ responsible under state law are the competent administrative authorities under competition law. Moreover, § 48 (2) sentence 2 GWB generally assigns responsibility to the highest state authorities. The Federal Cartel Office is responsible only if the law does not assign jurisdiction to a specific competition authority and the effect of a restrictive or discriminatory behaviour or a competition rule extends beyond the territory of one state, § 48 (2) sentence 1 GWB. § 49 (1) GWB also stipulates that both the Supreme State Authorities and the Federal Cartel Office are obliged to notify each other that proceedings have been initiated or investigations are being conducted. In accordance with § 49 (2)–(4) GWG, under certain circumstances, proceedings may also be transferred from the Supreme State Authority to the Federal Cartel Office (paragraphs (2) and (3)) or vice versa (paragraph (4)).

With regard to *sanctioning proceedings*, on the other hand, the procedure for imposing fines is generally governed by §§ 35 ff. OWiG. Regarding the procedure for imposing fines, §§ 81 ff. GWB are more specific provisions that take precedence in competition law. § 36 (1) no. 1 OWiG declares the authority responsible for the sanctioning proceedings to be the authority specified by law. Regarding this, § 82 GWB specifies the jurisdiction of the authorities in the area of competition law.³⁷ For other violations of § 81 GWB, the Federal Cartel Office and the – under state law responsible – Supreme State Authority are declared to be the competent authority for their respective areas of responsibility (§ 82 (1) no. 3 GWB).

³³ *Gesetz gegen Wettbewerbsbeschränkungen.*

³⁴ *Bundeskartellamt.*

³⁵ *Bundesministerium für Wirtschaft und Energie.*

³⁶ *Landeskartellbehörden.*

³⁷ Pursuant to § 82 (1) no. 1 GWB, the ‘*Bundesnetzagentur*’, as the market transparency body for electricity and gas, is the competent authority in particular for administrative offences pursuant to § 81 (2) no. 2 lit. c, d, no. 5a, 6 (in conjunction with § 47d (1) sentence 1 in conjunction with § 59 (2) or (4) GWB) and no. 8 (in conjunction with § 47d (1) sentence 1 in conjunction with § 59a (2) GWB). Pursuant to subsection 1 no. 2, the Federal Cartel Office, as the market transparency body for fuels, is the competent authority in particular for administrative offences pursuant to § 81 (1) no. 5b, 6 (in conjunction with § 47k (7) in conjunction with § 59 (2) or (4) GWB) and no. 8 (in conjunction with § 47k (7) in conjunction with § 59a (2) GWB).

1.5. Competent authorities in GDPR enforcement

The competence of the supervisory authority to impose an administrative fine pursuant to Art. 83 GDPR arises from Art. 55 (1) in conjunction with Art. 58 (2) lit. i GDPR. In Germany, this means that the authorities pursuant to the German federal states law³⁸ shall monitor the application by private bodies of data protection legislation within the scope of the GDPR in most cases. These are the state data protection commissioners in the individual states.³⁹ The Federal Commissioner shall be competent for businesses which process data of natural or legal persons for the commercial provision of telecommunications services, unless the responsibility for supervision is already indicated in § 29 of the Telecommunications Act ('TKG'⁴⁰), see § 9 (1) sentence 1 of the Federal Data Protection Act ('BDSG'⁴¹).

2. PUNITIVE ADMINISTRATIVE PROCEEDINGS: GENERAL FRAMEWORK

2.1. General remarks

2.1.1. Regulatory offences in German law

While criminal (procedural) law distinguishes between custodial sentences⁴² and fines,⁴³ regulatory offences only lead to administrative fines.^{44,45} The prosecution of regulatory offences is not led by the public prosecutor, instead the administrative body itself leads the investigation.⁴⁶ While in criminal proceedings only a court is competent to sentence a person to a punishment under criminal law, the administrative body decides whether to sanction an act or omission and on the sentencing. Only if that administrative decision is appealed, the question will be referred to the court

³⁸ *Landesrecht*.

³⁹ Only in Bavaria an additional separation of responsibility for the public sector and the non-public sector exists, see T. Born, '§ 8', in: L. Specht, R. Mantz (eds.), *Handbuch Europäisches und deutsches Datenschutzrecht*, Munich, Germany, C.H. Beck, 2019, § 7.

⁴⁰ *Telekommunikationsgesetz*.

⁴¹ *Bundesdatenschutzgesetz*.

⁴² *Freiheitsstrafe*.

⁴³ *Geldstrafe*.

⁴⁴ *Geldbuße*.

⁴⁵ Cf. D. Brodowski, 'Die Verwaltung darf nicht strafen – warum eigentlich nicht? Zugleich eine Vorstudie zu einer rechts-evolutionären, weichen Konstitutionalisierung strafrechtsdogmatischer Grundannahmen' *ZStW*, 2016, p. 370, 373, according to which there is always a prison sentence for criminal penalties, but never for administrative offences.

⁴⁶ U. Sieber, 'Administrative Sanction Law in Germany', p. 301, 316, in: M. Dyson, B. Vogel (eds.), *The Limits of Criminal Law – Anglo-German Concepts and Principles*, Cambridge, United Kingdom, Intersentia, 2018.

(see (d) below). In contrast to criminal law, therefore, the administrative body is – at least at first – the prosecuting and adjudicating body, § 35 (1), (2) OWiG.

The OWiG provides a general legal framework for administrative sanctions. The law on regulatory offences is to be distinguished from ‘core’ criminal law in the German legal system. § 1 (1) OWiG defines a regulatory offence as ‘an unlawful and reprehensible act, constituting the factual elements set forth in a statute that enables the act to be sanctioned by imposition of a regulatory fine’.

The formal distinction is therefore clear: if a statute calls for a sanction under criminal law (fine under criminal law or detention), it refers to ‘core’ criminal law; if it calls for a regulatory fine, it refers to the legal framework for administrative sanctions. However, the theoretical distinction between regulatory offence, on the one hand, and criminal offence, on the other hand, has been the subject of debate in criminal law for a long time.⁴⁷ Some⁴⁸ argue that the essential difference between regulatory offences and criminal offences is of a *qualitative* nature. While the law on regulatory offences is aimed at the impairment of institutional security and public services, the protective purpose of criminal law is the (individual) protection of legal interests.⁴⁹ Others do not want to recognise a qualitative, but rather a

⁴⁷ See the summary of the discussion in a historical review at D. Brodowski, ‘Quasi-criminal Enforcement Mechanisms in Germany: Past and Present’, p. 51, 66, in: V. Franssen, C. Harding (eds.), *Criminal and Quasi-criminal Enforcement Mechanisms in Europe (Franssen/Harding)*, Oxford, United Kingdom, Bloomsbury Publishing, Hart Studies in European Criminal Law Ser., 2022; Brodowski, (n. 45), *ZStW*, p. 372; Sieber, (n. 46), p. 323.

⁴⁸ For example P.J.A. von Feuerbach, C.J. Anton, *Lehrbuch des gemeinen in Deutschland gültigen peinlichen Rechts*, Aalen, Germany, Scientia, 1973 (reprint; original: 1847) (, § 432 p. 703, according to which criminal law protects individual interests and not collective interests; C.R. Köstlin, *System des deutschen Strafrechts – Abteilung 1 Allgemeiner Teil*, Aalen, Germany, Scientia, 1978, § 18 pp. 17 ff., who distinguishes between concrete endangerment or actual damage and merely abstract endangerment; J. Goldschmidt, *Das Verwaltungsstrafrecht – Eine Untersuchung der Grenzgebiete zwischen Strafrecht und Verwaltungsrecht auf rechtsgeschichtlicher und rechtsvergleichender Grundlage*, Berlin, Germany, Scientia, 1902, pp. 529 ff., J. Goldschmidt, ‘Begriff und Aufgabe des Verwaltungsstrafrechts’ *GA*, 1903, pp. 71, 84 ff., who distinguishes between wanting to be permitted and welfare of the administration; F. von Liszt, *Lehrbuch des deutschen Strafrechts*, Berlin, Germany, De Gruyter, 2nd ed., 1884, p. 102 and A. Merkel, *Lehrbuch des deutschen Strafrechts*, Stuttgart, Germany, Enke-Verlag, Juristische Handbibliothek, 1889, p. 45, who sees only disobedience in regulatory offences; but also E. Schmidt, *Das neue westdeutsche Wirtschaftsrecht – Grundsätzliches zu seiner Ausgestaltung und Anwendung*, Tübingen, Germany, Mohr-Siebeck, Deutsche Rechts-Zeitschrift, 1950, p. 44 f.

⁴⁹ S. Gerhold, ‘Introduction § 8’, in: J. Graf, *Beckscher Online-Kommentar zum OWiG (BeckOK OWiG)*, Munich, Germany, C.H. Beck, 43rd ed., 2024.

quantitative difference between the two types of offences.⁵⁰ Accordingly, a conceptual distinction is not possible. Rather, there is a quantitative difference depending on the amount of the monetary sanction.⁵¹

The Federal Constitutional Court⁵² ('BVerfG') advocates a mediating solution (so-called *Mixed-Qualitative-Quantitative Theory*), whereby a distinction is made according to qualitative aspects as a starting point. In doing so, the court recognises a socio-ethical or dishonourable unworthiness in criminal offences, so the imposition of an administrative fine does not appear sufficient. The regulatory offence is characterised by disobedience to the administration,⁵³ so an administrative fine is more likely imposed for the purpose of admonishing duties,⁵⁴ which, in particular, should not result in stigmatisation or impairment of a person's reputation.⁵⁵

From a systematic point of view, the OWiG is divided into three parts. While the first part (§§ 1–34 OWiG) contains general rules on the law of regulatory offences, the second part (§§ 35–110c OWiG) sets out the procedure for the imposition of regulatory fines. Finally, the third part (§§ 111–135 OWiG) deals with individual regulatory offences.⁵⁶ Although there are some obvious differences between the law on regulatory offences and criminal law, they also show far-reaching parallels.

On a general level, § 4 OWiG establishes the constitutional principles of *nulla poena sine lege* (§ 4 (1) OWiG) and *lex mitior* (§ 4 (3) OWiG); § 3

⁵⁰ Brodowski, (n. 45), *ZStW*, pp. 372 ff.; W. Knapp, 'Das Recht der Ordnungswidrigkeiten' *JuS*, 1979, p. 609, 610; A. Schoreit, 'Die sogenannten Ordnungswidrigkeiten', *GA*, 1967, pp. 225 ff.; W. Mitsch, *Recht der Ordnungswidrigkeiten*, Potsdam, Germany, Springer, 2nd ed., 2005, § 3 §§ 10 ff.; H. Mattes, *Untersuchungen zur Lehre von den Ordnungswidrigkeiten – Zweiter Halbband: Geltendes Recht und Kritik*, Berlin, Germany, Duncker & Humblot, 1982, pp. 46 f.; H.-H. Jescheck, 'Das deutsche Wirtschaftsstrafrecht' *JZ*, 1959, p. 457, 461; U. Weber, 'Die Überspannung der staatlichen Bußgeldgewalt – Kritische Bemerkungen zur neuen Entwicklung des materiellen Ordnungswidrigkeitenrechts' *ZStW*, 1980, p. 313, 316; J. Baumann, 'Über die notwendigen Veränderungen im Bereich des Vermögensschutzes' *JZ*, 1972, p. 1, 3; doubts regarding a qualitative distinction in P. Bockelmann, 'Literaturbericht Strafrecht – Besonderer Teil II', *ZStW*, 1954, p. 111, 124 f.

⁵¹ Cf. Brodowski, (n. 47), *Franssen/Harding*, p. 69.

⁵² *Bundesverfassungsgericht*.

⁵³ BVerfG, decision of 04.02.1959 – 1 BvR 197/53, *BVerfGE*, vol. 9, p. 167, 171.

⁵⁴ BVerfG, decision of 21.06.1977 – 2 BvR 70/75, 361/75, *BVerfGE*, vol. 45, p. 272, 289; decision of 16.07.1969 – 2 BvL 11/69, *BVerfGE*, vol. 27, p. 36, 42; decision of 16.07.1969 – 2 BvL 2/69, *BVerfGE*, vol. 27, p. 18, 33.

⁵⁵ BVerfG, decision of 16.07.1969 – 2 BvL 2/69, *BVerfGE*, vol. 27, p. 18, 33; critical of this approach Brodowski, (n. 45), *ZStW*, p. 370, 374 and D. Brodowski, 'Supranationale europäische Verwaltungssanktionen: Entwicklungslinien – Dimensionen des Strafrechts – Legitimität', pp. 139, 154 ff., in: K. Tiedemann, U. Sieber, H. Satzger, et al. (eds.), *Die Verfassung moderner Strafrechtspflege*, Baden-Baden, Germany, Nomos, Studien zum Wirtschaftsstrafrecht – Neue Folge, 2016.

⁵⁶ Sieber, (n. 46), p. 312.

OWiG upholds the guarantee of *nullum crimen sine lege*.⁵⁷ In addition, the person concerned must be treated as innocent until the end of the proceedings, they must be granted the right to be heard and the right to remain silent.⁵⁸ In particular, the principle of *fair trial* under Art. 6 (1) ECHR must also be observed.⁵⁹

In contrast to significant similarities, there are differences between the law on regulatory offences on the one hand and criminal procedure on the other as well, particularly regarding the legal consequences. One important difference is the *obligation* to prosecute punishable acts. While criminal proceedings follow the *principle of legality* (also known as principle of mandatory prosecution) (§ 152 (2) StPO) – which means law enforcement authorities must investigate whenever there is a suspicion of a criminal offence – the *principle of opportunity* is applied in the law on regulatory offences.⁶⁰ Accordingly, the prosecution of regulatory offences is at the discretion of the administrative body, § 47 (1) OWiG.

According to § 67 (1) OWiG, the person concerned can lodge an objection to an administrative fine within two weeks. It is a legal remedy in its own right and leads to a judicial review of the administrative decision.⁶¹ The objection has a suspensive effect (inhibiting effect), meaning the fine is not enforceable during the objection proceedings.⁶² The competent court is the district court in whose district the authority issuing the administrative act is based, § 68 (1) OWiG. Judicial review of the administrative act is therefore entrusted to the ordinary courts⁶³ in the context of regulatory offences, § 68 (1) OWiG;⁶⁴ the same court is also competent to decide matters relating to substantive criminal law. According to § 71 (1) OWiG, the court proceedings are generally governed by the provisions of the StPO.

A complaint on legal grounds may be lodged against a judgment under the conditions specified in § 79 (1) OWiG. Pursuant to § 121 (1) no. 1a of the Courts Constitution Act⁶⁵ ('GVG'), § 79 (3) sentence 1, § 80a in conjunction

⁵⁷ Brodowski, (n. 47), *Franssen/Harding*, p. 58; Sieber, (n. 46), p. 312.

⁵⁸ Sieber, (n. 46), p. 316.

⁵⁹ *Ibid.*, pp. 326 f.

⁶⁰ K. Krauß, in: H.-G. Kamann, S. Ohlhoff, S. Völcker (eds.), *Kartellverfahren und Kartellprozess*, § 18 § 31, Munich, Germany, C.H. Beck, 2017.

⁶¹ OLG Düsseldorf, decision of 17.08.1999 – 5 Ss (OWi) 339/98, § 18; K. Ellbogen, '§ 67' in: W. Mitsch (ed.), *Karlsruher Kommentar zum Gesetz über Ordnungswidrigkeiten* (KK-OWiG), Munich, Germany, C.H. Beck, 5th ed., 2018, § 1.

⁶² Ellbogen, (n. 61), § 3.

⁶³ *Amtsgericht*.

⁶⁴ Ellbogen (n. 61), § 20.

⁶⁵ *Gerichtsverfassungsgesetz*.

with § 46 (7) OWiG, the court of appeal is the Higher Regional Court ('OLG'⁶⁶) with local jurisdiction.⁶⁷

2.1.2. General framework for gathering evidence from third parties in regulatory offence proceedings

Unless otherwise provided by the OWiG, the provisions of the general laws concerning criminal proceedings, particularly the StPO, shall apply *mutatis mutandis* to the regulatory sanctioning proceedings.⁶⁸ The wording of § 46 (1) OWiG itself clarifies that the standards for prosecuting criminal offences and administrative offences are not identical. This may lead to some provisions of the StPO not being applicable in full. By outlining the limitations of the OWiG reference to the StPO as well as the limitations regarding the third parties' competences to disclose information, a general framework for gathering evidence from third parties in German administrative proceedings can be derived.

§ 46 OWiG itself restricts the referral to the StPO in its (3) to (5), which list several measures that may not, or not in their entirety, be undertaken in the case of investigating and prosecuting a regulatory offence, as well as some provisions that are not to be applied fully. Confiscation of postal items and telegrams,⁶⁹ as well as requests for information regarding matters that are subject to post and telecommunications secrecy,⁷⁰ shall be inadmissible.⁷¹ Therefore, telecommunications surveillance⁷² as well as traffic data capture⁷³ are explicitly excluded from regulatory offence proceedings by § 46 (3) OWiG.⁷⁴ Some consider the exclusions in § 46 (3) to (5) OWiG to be

⁶⁶ *Oberlandesgericht*.

⁶⁷ A. Hadamitzky, 'preliminary remarks §§ 79 ff.' in: W. Mitsch (ed.), *KK-OWiG*, Munich, Germany, C.H. Beck, 5th ed., 2018, § 1.

⁶⁸ § 46 (1) OWiG.

⁶⁹ §§ 99, 100 StPO.

⁷⁰ Art. 10 (1) of the Basic Law (*Grundgesetz*, 'GG'), i.e. the German constitution.

⁷¹ § 46 (3) sentence 1 OWiG.

⁷² § 100a StPO.

⁷³ § 100g StPO.

⁷⁴ § 46 (3) OWiG applies to traffic data as well. The reason for this is that the protection granted by Art. 10 (1) GG extends not only to the content of telecommunication, but also to its circumstances, see BVerfG, decision of 20.06.1984 – 1 BvR 1494/78, *BVerfGE*, vol. 67, p. 157, 172; judgment of 14.07.1999 – 1 BvR 2226/94 and others, *BVerfGE*, vol. 100, p. 313, 358; judgment of 12.03.2003 – 1 BvR 330/96, 348/99, *BVerfGE*, vol. 107, p. 299, 312 f.; judgment of 02.03.2010 – 1 BvR 256/08 and others, *BVerfGE*, vol. 125, p. 260, 309; decision of 24.01.2012 – 1 BvR 1299/05, *BVerfGE*, vol. 130, p. 151, 179; C. Rückert, '§ 100g', in: C. Knauer, H. Kudlich, H. Schneider (eds.), *Münchener Kommentar zur StPO* (MüKo-StPO), Munich, Germany, C.H. Beck, 2nd ed., 2023, § 12.

exhaustive.⁷⁵ This cannot be agreed with, particularly in view of the limiting wording in the StPO.

For instance, for some investigative measures, a catalogue⁷⁶ of specific offences is set out, meaning that the corresponding measure may only be taken in the case of precisely these offences. Additionally, if a provision in German criminal procedure was ‘introduced to combat organised crime’, it cannot be applied analogously in regulatory offence proceedings, as this would otherwise contradict the expressly manifested legislative intent – regardless of whether it refers to specific criminal offences or not.⁷⁷ In a similar vein, all provisions of the StPO that apply only to ‘criminal offences of substantial significance’⁷⁸ are inapplicable in administrative fine proceedings.⁷⁹ Restrictions of such nature apply to the covert seizure of an object that a third party has in their custody⁸⁰ – therefore, the person accused of the regulatory offence always has to be notified of the seizure of an object from a third party –, to dragnet investigations,⁸¹ to technical investigation measures in respect of mobile terminals,⁸² to requests of passwords or other login data from digital services,⁸³ as well as – generally – to the capture of usage data in respect to digital service providers.⁸⁴

In general, it can be said that the reference in § 46 OWiG is ‘doubly imprecise’, as it not only refers – almost entirely – to the StPO, but also immediately restricts this by adding ‘*mutatis mutandis*’.⁸⁵ Painting with a

⁷⁵ J. Lampe ‘§ 46’, in: W. Mitsch (ed.), *KK-OWiG*, Munich, Germany, C.H. Beck, 5th ed., 2018, § 13.

⁷⁶ See for example § 100a (2) of the StPO.

⁷⁷ Regarding § 100h StPO (Other measures outside of private premises) T. Elsner, ‘Video- und Bildaufnahmen zur Abstandsmessung im Straßenverkehr – nicht ohne eine Rechtsgrundlage’ *DAR*, 2010, p. 163, 166.

⁷⁸ *Erhebliche Bedeutung*.

⁷⁹ LG Bonn, decision of 14.01.2005 – 32 Qs 5/05, *NSiZ*, 2005, p. 528; M. Bauer, ‘§ 46’, in: M. Bauer, A. Thoma (eds.), *Göhler, Ordnungswidrigkeitengesetz*, Munich, Germany, C.H. Beck, 19th ed., 2024, § 8.

⁸⁰ § 95a StPO.

⁸¹ § 98a StPO.

⁸² § 100i StPO. It can therefore be left up for debate whether the gathered data actually falls under Art. 10 (1) GG and § 46 (3) OWiG, cf. BVerfG, decision of 22.08.2006 – 2 BvR 1345/03, *NJW*, 2007, p. 351, which denied an encroachment on Art. 10 (1) GG; C. Rückert, ‘§ 100i’, in: C. Knauer, H. Kudlich, H. Schneider (eds.), *MüKo-StPO*, Munich, Germany, C.H. Beck, 2nd ed., 2023, § 18, who argues in favour of a protection by Art. 10 (1) GG.

⁸³ § 100j (1) sentence 2 StPO. Note that this restriction does not extend to login data gathered from telecommunication services (§ 100j (1) sentence 2 StPO).

⁸⁴ § 100k (1), (2) StPO.

⁸⁵ B. Dietrich, *Die Bindung des Bußgeldverfahrens an das Strafverfahrensrecht: Eine Studie zu Notwendigkeit und Grenzen des § 46 Abs. 1 OWiG – zugleich ein Beitrag zum Schweigerecht des Betroffenen*, Baden-Baden, Germany, Nomos, 2003, pp. 124 f. prevention

broad brush, the interpretations here range from a standard formulation of analogue⁸⁶ application to a restrictive⁸⁷ application. It must be conceded that the formulation of *mutatis mutandis* (or similar) must always be supplemented ‘if the reference text does not fit literally’ (so-called analogy reference).⁸⁸ It is therefore not clear that this is associated with a restriction from the outset. However, purpose and comparability must always be considered, even beyond the specific grounds for exclusion. Particularly in the case of investigative measures, this can also be done dogmatically in the context of proportionality so that an assessment of the circumstances of the individual case must take place.⁸⁹

When weighing up the interests involved, it must be considered that the ‘severity’ of administrative offences is by many perceived as lower than that of criminal offences.⁹⁰ So the classification as a ‘mere administrative offence’ is justified by the fact that ‘the accusation of a criminal offence is always more serious than that of an administrative offence’.⁹¹ However, it is also worth noting that the amount to be paid as an administrative fine increasingly exceeds the amount of the fines incurred by criminal offences. ‘Taking into account the different weight of offences subject to criminal law and offences subject to fines and the associated different depth of sanctions, a decision must be made as to *whether* certain powers of intervention can also be applied in administrative fine proceedings.’⁹² Consequently, the level of the sanction for the offence committed and the severity of the specific power to encroach on fundamental rights are decisive factors for the question of the applicability

of any recourse to the StPO if there are special regulations in the OWiG; LG Bonn, decision of 14.01.2005 – 32 Qs 5/05, *NStZ*, 2005, p. 528; A. Rebler, ‘Durchsuchung und Beschlagnahme im Bußgeldverfahren’ *SVR*, 2014, p. 41, 42 not applicable *per se* so different severity of offences under criminal law and administrative sanctioning must be taken into account.

⁸⁶ LG Berlin, decision of 18.02.2021 – (526 OWi LG) 212 Js-OWi 1/20 (1/20), § 18, juris; referring to: Bundesministerium der Justiz, *Handbuch der Rechtsförmlichkeit*, Cologne, Germany, 3rd ed., 2008, §§ 218 ff., 232 ff. – common reference to laws that are not identical in wording, but there is ‘no indication that the provisions of the administrative offences act would be “limited” or even selectively not applicable at all’ [own translation].

⁸⁷ *Ibid.*, pp. 123.

⁸⁸ Bundesministerium der Justiz, (n. 86), § 232.

⁸⁹ A. Bücherl, ‘§ 46’, in: J. Graf (ed.), *BeckOK OWiG*, Munich, Germany, C.H. Beck, 43rd ed., 2024, § 4; Rebler, (n. 85), p. 42.

⁹⁰ Bücherl, (n. 89), § 2; L. Firchau ‘§ 410 AO’, in: D. Gosch, A. Hoyer (eds.), *Abgabenordnung Finanzgerichtsordnung*, Bonn, Germany, Stollfuß, 184th ed., 2024, § 16; Bauer, (n. 79), § 10; Rebler, (n. 85), p. 42; E. Kraatz, *Ordnungswidrigkeitenrecht*, Baden-Baden, Germany, Nomos, 2nd ed., 2023, § 13 §§ 9, 13.

⁹¹ Bauer, (n. 79), § 10.

⁹² LG Bonn, decision of 14.01.2005 – 32 Qs 5/05, *NStZ*, 2005, p. 528 [own translation, emphasis here]; in this direction also Dietrich, (n. 85), p. 210: ‘The state’s access to the person concerned must be limited in accordance with the weight of the sanction.’ [own translation].

of the respective standard. Moreover, an enquiry to a company can have a revealing effect and thus create an intrusion into the privacy of the person concerned. This applies in particular if data requests by law enforcement authorities to certain providers and in relation to certain data are not part of everyday business and are therefore suspicious. Proportionality is not rejected from the outset in the case of administrative offences.⁹³ ‘However, the less serious the offence with which the person concerned is charged, the higher the requirements for the strength of the suspicion. [...] Accordingly, [...] a weak initial suspicion requires a strict proportionality test.’⁹⁴ ‘In any case, there is no systematic lower limit for more intensive intervention measures, for example with regard to the amount of the fine; rather, a balance must be struck in each individual case.’⁹⁵

Lastly, some measures are not excluded based on the law of regulatory offence procedure, but based on the law governing the OSPs. According to the so-called double-door model^{96,97} ‘the corresponding interventions of retrieval and transmission [...] each require their own legal basis’. The double-door model applies not only to the exchange of data between two public authorities, but also to the exchange of data between a private service provider on the one hand and a public authority seeking information on the other.⁹⁸ Both ‘doors’ may be manifested in the same legal basis.⁹⁹ A distinction must therefore always be made between the normative prerequisite for requesting the data on the one hand and the disclosure of the data on the other. Only if both ‘doors’ are ‘open’, the data transfer is lawful. In particular, a usage data request for the sole purpose of identifying the user,¹⁰⁰ which is exempt from

⁹³ BVerfG, Chamber’s order of 14.07.2016 – 2 BvR 2748/14, § 34, juris; decision of 27.07.2007 – 2 BvR 1994/02; see also on tax matters BVerfG, decision of 09.03.2005 – 2 BvR 1178/04, *BeckRS*, 2005, 2460.

⁹⁴ BVerfG, decision of 27.07.2007 – 2 BvR 1994/02.

⁹⁵ BVerfG, Chamber’s order of 14.07.2016 – 2 BvR 2748/14, § 34, juris; decision of 27.07.2007 – 2 BvR 1994/02; C. Krumm, ‘BVerfG: Durchsuchung wegen Identifizierung nach VerkehrsOWi mit 80 Euro Geldbuße ist unverhältnismäßig!’ *beck blog*, 2016, online <https://community.beck.de/2016/08/30/bverfg-durchsuchung-wegen-identifizierung-nach-verkehrsowi-mit-80-euro-geldbusse-ist-unverhaeltnismaessig> [own translation].

⁹⁶ *Doppeltürmodell*.

⁹⁷ BVerfG, decision of 24.01.2012 – 1 BvR 1299/05, *NJW*, 2012, p. 1419, 1423 § 123 [own translation]; also referred to in the figurative ‘double door’; BVerfG, decision of 27.05.2020 – 1 BvR 1873/13, 2618/13, *NJW*, 2020, p. 2699, 2701; decision of 18.12.2018 – 1 BvR 142/15, *NJW*, 2019, p. 827, 833 § 80; judgment of 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, *NJW*, 2016, p. 1781, 1803 § 305; decision of 06.03.2014 – 1 BvR 3541/13 and others, *NJW*, 2014, p. 1581 § 18; decision of 24.01.2012 – 1 BvR 1299/05, *NJW*, 2012, p. 1419, 1423 § 123.

⁹⁸ VGH Munich, decision of 20.05.2020 – 12 B 19.1648, *BeckRS*, 2020, 10398 § 47.

⁹⁹ *Pars pro toto*, see D. Brodowski, *Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht*, Tübingen, Deutschland, Mohr Siebeck, 2016, p. 137.

¹⁰⁰ § 100k (3) StPO.

the restrictions of a regular capture of usage data,¹⁰¹ is barred in practice as digital service providers are only allowed to disclose that information for the purposes of criminal, not regulatory offence investigations.¹⁰² The same applies to a subscriber data request referencing an IP address at a specific point in time.¹⁰³

However, there are still some legal means the administration can rely on to request electronic evidence from private actors.

Firstly, apart from postal items and telegrams, objects may be secured and seized for evidentiary purposes and third parties may be obligated to surrender such objects.¹⁰⁴

Secondly, subscriber data – apart from digital services login data – may be requested, though this is limited to such offences on which maximum fines of more than 15.000 € are imposable on natural persons insofar as it concerns digital services.¹⁰⁵

Thirdly, the general clause for investigations¹⁰⁶ covers the competence of the administration to demand, either by itself or through the police authorities and police officers, any kind of information concerning the case

¹⁰¹ § 100k (3) StPO dispenses the authorities not only from the need of a court decision, but also from all of the other requirements of § 100k (1), (2) StPO like that of a suspicion of specific crimes, cf. B. Gercke, A. Grözinger, ‘§ 100k’, in: B. Gercke, D. Temming, M.A. Zöller (eds.), *StPO*, Heidelberg, Germany, C.F. Müller, 7th ed., 2023, § 10.

¹⁰² § 24 (3) no. 1, (1) sentence 1 of the Telecommunications and Digital Services Data Protection Act – *Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz*, ‘TDDDG’. Since any request of usage data is therefore inapplicable, it is inconsequential for the purpose of this report whether the usage of digital services actually falls under the provision of Art. 10 (1) GG and therefore § 46 (3) OWiG; cf. C. Rückert, ‘§ 100k’, in: C. Knauer, H. Kudlich, H. Schneider (eds.), *MüKo-StPO*, Munich, Germany, C.H. Beck, 2nd ed., 2023, § 4, who argues in favour of a protection by Art. 10 (1) GG.

¹⁰³ § 100j (2), (1) sentence 1 no. 1, no. 2 StPO in conjunction with § 174 (5) no. 1, (1) sentence 3, § 177 (1) no. 3 TKG, § 22 (4) no. 1, (1) sentence 3 TDDDG – see below in detail. The BVerfG has ruled that such requests of subscriber data on the basis of a specific IP address constitute an interference of considerable weight with the privacy of telecommunication, as they require access to telecommunications traffic data. Therefore, they may not generally be permitted to prosecute any kind of administrative offence, but only ones ‘of particular weight – including in the individual case’ – and ‘expressly specified by the legislator’ (BVerfG, judgment of 02.03.2010 – 1 BvR 256/08 and others, *BVerfGE*, vol. 125, p. 260, 344; cf. also decision of 27.05.2020 – 1 BvR 1873/13, *BVerfGE*, vol. 155, p. 119, 200 f.). However, in absence of a corresponding authorisation of the OSP, it is not necessary to decide whether the restriction based on the amount of the potential fine in § 46 (4a) OWiG fulfils the requirement of an express specification.

¹⁰⁴ § 46 (2) OWiG in conjunction with §§ 94, 95 StPO.

¹⁰⁵ § 46 (2) OWiG in conjunction with § 100j StPO, § 46 (4a) OWiG.

¹⁰⁶ § 46 (2) OWiG in conjunction with §§ 161, 163 StPO.

from all authorities. Private actors, on the other hand, can generally only be asked to provide information, without them being obliged to comply.¹⁰⁷

2.1.3. General characteristics of these requests

With regard to the legal protection of persons concerned by requests and the remedies available to them as well as to the OSPs, German law provides a general framework. In German criminal proceedings – and therefore also in regulatory offences proceedings – parties to the proceedings¹⁰⁸ are entitled to the right to be heard.¹⁰⁹ For court decisions outside a main hearing, this means that the accused person has to be heard before evidence is used to their detriment.¹¹⁰ Additionally, not only the accused person but also anyone else affected by a court decision¹¹¹ has to be notified of any decision relating to them.¹¹² However, as regards decisions that the public prosecution or the police is competent to make on their own, there is no general obligation to notify the accused person of such decisions.¹¹³ For some investigation measures like specific subsets of subscriber data requests¹¹⁴ and capture of usage data,¹¹⁵ there are special notification duties in place.

The available remedy against an investigation measure is dependent on the responsible authority: Court orders can be proceeded against with a complaint.^{116,117} Primarily, all parties to the proceedings are entitled to a complaint, including the accused person.¹¹⁸ Whoever complains needs to be

¹⁰⁷ R. Kölbel, V. Ibold, ‘§ 161’, in: C. Knauer, H. Kudlich, H. Schneider (eds.), *MüKo-StPO*, Munich, Germany, C.H. Beck, 2nd ed., 2024, § 26.

¹⁰⁸ H. Larcher, ‘§ 33’, in: J. Graf (ed.), *BeckOK StPO mit RiStBV und MiStra* (BeckOK StPO), Munich, Germany, C.H. Beck, 52nd ed., 2024, § 5.

¹⁰⁹ B. Valerius, ‘§ 33’, in: C. Knauer, H. Kudlich, H. Schneider (eds.), *MüKo-StPO*, Munich, Germany, C.H. Beck, 2nd ed., 2023, § 1.

¹¹⁰ § 33 (3), (2) StPO.

¹¹¹ H. Larcher, ‘§ 35’, in: J. Graf (ed.), *BeckOK StPO*, Munich, Germany, C.H. Beck, 52nd ed., 2024 § 2.

¹¹² § 35 (2), (1) StPO.

¹¹³ Cf. H. Schneider-Glockzin, ‘§ 35’, in: C. Barthe, J. Gericke (eds.), *Karlsruher Kommentar zur Strafprozessordnung* (KK-StPO), Munich, Germany, C.H. Beck, 9th ed., 2023, § 2; T. Ziegler, ‘§ 35’, in: B. von Heintschel-Heinegg, J. Bockemühl (eds.), *KMR-StPO*, Hürth, Germany, Carl Heymanns, 130th ed., 2024, § 2.

¹¹⁴ § 100j (4) StPO.

¹¹⁵ § 101a (7) StPO.

¹¹⁶ *Beschwerde*.

¹¹⁷ §§ 304 ff. StPO. See also B. Krenberger, C. Krumm, *OWiG*, Munich, Germany, C.H. Beck, 8th ed., 2024, § 62 § 11; K.-H. Kurz, ‘§ 62’, in: W. Mitsch (ed.), *KK-OWiG*, Munich, Germany, C.H. Beck, 5th ed., 2018, § 3.

¹¹⁸ S. Neuheuser, ‘§ 304’, in: C. Knauer, H. Kudlich, H. Schneider (eds.), *MüKo-StPO*, Munich, Germany, C.H. Beck, 2nd ed., 2024, § 34.

affected¹¹⁹ in their rights or legitimate interests by the contested decision,¹²⁰ e.g. due to a third party being obligated to disclose personal data on them. The complaint is to be lodged at the court whose decision is being contested, which may then redress it or submit it to another court hearing the complaint.¹²¹ Against a measure ordered by the administrative authority, the person concerned may file a request for a court decision.¹²² The court decision, however, cannot be contested in turn unless otherwise provided by statute.¹²³ In case of a decision of the police, the request arguably cannot be made directly; rather, the person concerned has to appeal to the administration authority first and can only then contest the administration authority's confirmation of the police's actions.¹²⁴ As an exception, measures taken only for the preparation of the final decision are excluded.¹²⁵ This requires the measure to have no significance by itself and to not interfere with any person's legal sphere,¹²⁶ which cannot be said for any of the investigation measures discussed here. According to some, the person concerned may only make a request against a decision directed against them.¹²⁷ This could be read to mean that there would be no remedy available against a request concerning a third party. However, such a remedy might be possible in case of a legitimate interest,¹²⁸ e.g. when personal data of the person concerned is disclosed; this is also accepted in case of criminal proceedings.¹²⁹

There are no special remedies available to the private actors. Rather, they can make use of the remedies discussed above. In case of a decision of the administrative authority, the private actor obligated to surrender an object or information can apply for a court decision,¹³⁰ as they are another 'person

¹¹⁹ *Betroffen*.

¹²⁰ § 304 (2) StPO; see also P. Reichenbach, '§ 296', in: B. Gercke, D. Temming, M.A. Zöller (eds.), *StPO*, Heidelberg, Germany, C.F. Müller, 7th ed., 2023, § 12.

¹²¹ § 306 (1), (2) StPO.

¹²² § 62 (1) OWiG.

¹²³ This is made clear by § 62 (2) OWiG. In this respect, the proceedings diverge from those in criminal matters, where generally § 98 (2) sentence 2 StPO would be the given remedy, cf. K. Gassner, '§ 62', in: K. Gassner, S. Seith (eds.), *OWiG*, Baden-Baden, Germany, Nomos, 2nd ed., 2020, § 3.

¹²⁴ Kurz, (n. 117), § 3; cf. also Krenberger, Krumm, (n. 117), § 62 § 6; differently Gassner, (n. 123), § 7.

¹²⁵ § 62 (1) sentence 2 OWiG.

¹²⁶ Kurz, (n. 117), § 7.

¹²⁷ Krenberger, Krumm, (n. 117), § 62 § 16; M. Euler, '§ 62', in: J. Graf (ed.), *BeckOK OWiG*, Munich, Germany, C.H. Beck, 43rd ed., 2024, § 11.

¹²⁸ This is at least not precluded by the wording of § 62 (1) sentence 1 OWiG.

¹²⁹ E.g. as regards §§ 100j, 98 (2) sentence 2 StPO, see J. Graf, '§ 100j', in: J. Graf (ed.), *BeckOK StPO*, Munich, Germany, C.H. Beck, 52nd ed., 2024, § 40; C. Rückert, '§ 100j', in: C. Knauer, H. Kudlich, H. Schneider (eds.), *MüKo-StPO*, Munich, Germany, C.H. Beck, 2nd ed., 2023, § 72.

¹³⁰ § 62 (1) sentence 1 OWiG.

against whom the measure is directed'.¹³¹ As for court decisions, it is debatable whether the complaint under §§ 304 ff. StPO is applicable with reference to a third party like the private actor requested in these cases. Generally, according to § 304 (2) StPO, the complaint is not limited to the parties to the proceedings, but may also be lodged by witnesses, experts and other persons against orders that affect them, e.g., the holder of an object is affected by a seizure.¹³²

2.2. Specific request for data to online service providers: subscriber data request

The various restrictions detailed above leave only one legal basis for requests specifically targeting OSPs in cases of regulatory offences, namely the subscriber data request (§ 46 (2) OWiG in conjunction with § 100j StPO).

2.2.1. Definition of OSP

This requests targets two different types of OSPs, the first of which being telecommunications services.¹³³ It can be made to any person who, on a commercial basis, provides or collaborates in the provision of telecommunications services. The definition of 'telecommunications services' is nearly identical to that of 'electronic communications services' in Art. 2 (4) of the European Electronic Communications Code except for its focus on 'telecommunication' instead of 'electronic communication':¹³⁴ 'a service normally provided for remuneration via telecommunications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using telecommunications networks and services, the following types of services: (a) internet access services; (b) interpersonal telecommunications services; and (c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting'.¹³⁵

Besides telecommunication service providers, digital service providers can also be requested to surrender subscriber data.¹³⁶ This obligation extends to any person who, on a commercial basis, makes digital services available

¹³¹ Cf. Euler, (n. 127), § 12 with regard to search and seizure.

¹³² Neuheuser, (n. 118), § 36.

¹³³ § 100j (1) sentence 1 no. 1 StPO. The corresponding legal basis authorising OSPs to disclose this information can be found in § 174 TKG.

¹³⁴ Directive (EU) 2018/1972 of the European Parliament and of the Council of 11.12.2018 establishing the European Electronic Communications Code.

¹³⁵ § 3 no. 61 TKG.

¹³⁶ § 100j (1) sentence 1 no. 2 StPO. § 22 TDDDG contains the corresponding legal basis for the OSP to disclose this information.

for use or provides access for the purpose of the use of their own or others' digital services. 'Digital service' is defined¹³⁷ as identical to the term 'service' as defined in Art. 1 (1) (b) of the Directive (EU) 2015/1535,¹³⁸ meaning an Information Society service. This in turn is defined as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.'

2.2.2. Type of data or information that can be requested

With regard to telecommunications services, this request relates to *subscriber data*. On the one hand, it refers to data that telecommunication providers are required by law¹³⁹ to gather and save in order to enable corresponding demands by the authorities. These data are: telephone numbers, other identifiers assigned by them, name and address of the subscriber, in case of a natural person their date of birth, in case of a landline its address, in case a phone is provided alongside a mobile connection its device number, and the date of assignment of the telephone number as well as the date of commencement of the contract, if they differ. On the other hand, it refers to any subscriber data collected by the telecommunication service without being required to do so. Subscriber data are defined as the data of an end user which are required for the foundation, configuration, adjustment, or termination of a contractual relationship concerning telecommunication services.¹⁴⁰ They include, as a subset, data by means of which access to terminals or to storage media installed in such terminal equipment or physically separated therefrom are protected (*login data*).¹⁴¹ Those include usernames, passwords, cryptographic keys, Personal Identification Numbers

¹³⁷ § 2 (1) TDDDG in conjunction with § 1 (4) no. 1 of the German Digital Services Act (*Digitale-Dienste-Gesetz*, 'DDG').

¹³⁸ Directive (EU) 2015/1535 of the European Parliament and of the Council of 09.09.2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

¹³⁹ § 172 (1) TKG (§ 174 (1) sentence 1 TKG).

¹⁴⁰ § 3 no. 6 TKG.

¹⁴¹ This follows from § 174 (1) sentence 2 TKG.

(PIN) and Personal Unlocking Keys (PUK).¹⁴² In the absence of a provision limiting its personal scope, the request may extend not only to subscriber data of the accused person, but also to data belonging to anyone else.

With regard to digital services, *subscriber data* is defined as the personal data whose processing is required for the foundation, configuration, or adjustment of a contractual relationship between the provider of digital services and the user concerning the use of digital services.¹⁴³ Contrary to requests from telecommunications service providers, as an especially protected subset of subscriber data, passwords collected in the form of subscriber data or other data which are used to provide protection against access to end devices or to storage devices which are used in or kept separate from such end devices (*login data*)¹⁴⁴ cannot be requested in an investigation of a regulatory offence.¹⁴⁵ As with requests to telecommunications services, the scope is not limited to data of the accused person.

2.2.3. Conditions to request data

Several conditions are set up to restrict such a request: Firstly, there needs to be an initial suspicion of a regulatory offence. Secondly, the information has to be necessary to establish the facts or to determine the whereabouts of an accused person. It does not matter whether the requested subscriber data belongs to the accused person or a third party.¹⁴⁶ The regular subscriber data request does not require a court order and can be ordered by the public prosecutor's office or the police;¹⁴⁷ in regulatory offence proceedings, it can therefore be ordered by the administrative authority. A subsequent court confirmation is not necessary. Like any investigative measure, the request needs to be proportional. As a further restriction for requests to digital service providers, data may only be requested to prosecute a regulatory offence for which regulatory fines that exceed 15.000 euros can be imposed on natural persons.¹⁴⁸

§ 100j (2) StPO clarifies that a subscriber data request for the purpose of prosecuting criminal offences may also reference an Internet Protocol (IP) address at a specific point in time; this clarification was necessary as the BVerfG had ruled that such a request referring to a dynamic IP address

¹⁴² D. Brodowski, 'StPO § 100j', in: G. Borges, M. Hilber (eds.), *BeckOK IT-Recht*, Munich, Germany, C.H. Beck, 15th ed., 2024, § 6.

¹⁴³ § 2 (2) no. 2 TDDDG (§ 22 (1) sentence 1 TDDDG).

¹⁴⁴ § 22 (1) sentence 2, § 23 TDDDG.

¹⁴⁵ § 100j (1) sentence 3 StPO.

¹⁴⁶ Brodowski, (n. 142), § 13.

¹⁴⁷ § 100j (3) StPO implicitly states this; see also L. Greco, '§ 100j', in: J. Wolter, M. Deiters (eds.), *SK-StPO*, Hürth, Germany, Carl Heymanns, 6th ed., 2023, § 16.

¹⁴⁸ § 46 (4a) OWiG.

encroaches on the fundamental right to telecommunications secrecy.¹⁴⁹ With regard to investigations of regulatory offences, § 46 (3) sentence 1 StPO may be read in accordance with the BVerfG¹⁵⁰ as precluding any measure encroaching on the right to telecommunications secrecy, and therefore also this subset of subscriber data request.¹⁵¹ However, even if this provision did not preclude such a request, with respect to telecommunications services § 174 (5) no. 1, (1) sentence 3 TKG only authorises OSPs to disclose such data to authorities investigating criminal offences, not ones investigating regulatory offences. With regard to digital service providers, even though § 46 (4a) OWiG declares § 100j (1) sentence 1 no. 2 StPO to be applicable ‘also in conjunction with § 100j (2) StPO’ and therefore including requests referencing IPs at a specific point in time,¹⁵² § 22 (4) no. 1, (1) sentence 3 TDDDG does not authorise OSPs to disclose that kind of data to authorities prosecuting regulatory offences, but only to such prosecuting criminal offences.¹⁵³ This discrepancy between the administrative body’s legal authority and the OSP’s authorisation makes such a request illegal. Using the BVerfG’s double door metaphor, while the door of data collection on the side of the authorities is open, the door of transmission on the side of the private person is closed. Hence, a subscriber data request may not reference an IP address at a specific point in time, regardless of which type of OSP the request targets.

Additional requirements are in place with respect to requests of login data from telecommunications service providers. Such data may only be requested if the statutory requirements for its use are met.¹⁵⁴ Although increasingly challenged,¹⁵⁵ the use of login data by the authorities to unlock

¹⁴⁹ BVerfG, decision of 24.01.2012 – 1 BvR 1299/05, *BVerfGE*, vol. 130, p. 151, 181 f.; decision of 27.05.2020 – 1 BvR 1873/13, 2618/13, *BVerfGE*, vol. 155, p. 119, 169.

¹⁵⁰ BVerfG, decision of 27.05.2020 – 1 BvR 1873/13, 2618/13, *BVerfGE*, vol. 155, p. 119, 204.

¹⁵¹ Against such a reading, it might be argued that, strictly adhering to the wording of § 46 (3) OWiG, the requested information is not actually protected by Art. 10 (1) GG, even though the request encroaches on this fundamental right.

¹⁵² On the basis of the wide interpretation of § 46 (3) OWiG, the provision of § 46 (4a) OWiG may be seen as *lex specialis*.

¹⁵³ Cf. also K. Schreiber, ‘TTDSG § 22’, in: M. Geppert, R. Schütz (eds.), *Beck’scher TKG-Kommentar*, Munich, Germany, C.H. Beck, 5th ed., 2023, § 46; D. Ettig, ‘TTDSG § 22’, in: J. Taeger, D. Gabel (eds.), *DSGVO – BDSG – TTDSG*, Frankfurt am Main, Germany, dfv, 4th ed., 2022, § 18.

¹⁵⁴ § 100j (1) sentence 2 StPO.

¹⁵⁵ M. El-Ghazi, *Beschlagnahme und Auswertung von Handys, Laptops & Co. – Sind beim offenen Zugriff auf Datenträger die Persönlichkeitsrechte angemessen geschützt?*, Munich, Germany, C.H. Beck, 2024, Gutachten C zum 74. Deutschen Juristentag, p. C50 ff.; D. Brodowski, ‘Durchsuchung, Durchsicht und Beschlagnahme bei informationstechnischen Systemen’ *Juristenzeitung*, 2024, p. 750, 752 f.

devices is justified by many on the basis of the existing legislation¹⁵⁶ and therefore is subject to no substantial further restrictions beyond that the device to be unlocked may be of importance as evidence to the case. The concerned person has to be notified of the disclosure of their data only in case of a request of login data and only as soon as it does not circumvent the purpose of the measure.¹⁵⁷ A login data request from telecommunications services requires a court order.¹⁵⁸ As an exception, this is not the case in exigent circumstances, though a court decision has to be sought without delay.¹⁵⁹ As an exception to the exception, a court order is not required if the subject already has or must have knowledge or if the use of the data has already been permitted by court decision.¹⁶⁰

2.2.4. Rules on the transfer of data

For telecommunications services, the rules of transfer of data are the following.¹⁶¹ While there is no hard deadline, the provider is required to transmit the data without delay and completely.¹⁶² It is required to take into account any source of data internal to the company and to take the arrangements necessary for disclosure at one's own expense. The obligated party has to maintain silence about the request with regard to the concerned party as well as third parties. The law determines that companies providing publicly available telecommunications services are required to keep available a secure electronic interface for receiving requests as well as sending the required information;¹⁶³ further and more specific requirements on this interface are laid down in statutory instruments¹⁶⁴ of the federal government.¹⁶⁵ These provisions specify two ways to answer a request.

¹⁵⁶ More specifically, on the basis of § 94 StPO as an annex to the seizure of such devices or by the general clause of §§ 161, 163 StPO, see Brodowski, (n. 142), § 14.

¹⁵⁷ § 100j (4) StPO.

¹⁵⁸ § 100j (3) sentence 1, (1) sentence 2 StPO.

¹⁵⁹ § 100j (3) sentences 2, 3 StPO.

¹⁶⁰ § 100j (4) sentence 4 StPO.

¹⁶¹ They are laid down in § 100j (5) as well as § 174 (1), (6), (7) TKG.

¹⁶² § 100j (5) StPO, § 174 (1) sentences 4, 5, (6) TKG.

¹⁶³ § 174 (7) TKG.

¹⁶⁴ *Rechtsverordnungen*.

¹⁶⁵ § 174 (7) in conjunction with § 170 (5), (6) TKG allow the executive branch to regulate the specifics by statute. The relevant norms are §§ 30–35 of the Statutory instrument on the implementation of measures for the surveillance of telecommunication (*Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation*, ‘TKÜV’), as well as Chapter B of the Technical guideline for the implementation of legal measures for the surveillance of telecommunication, disclosure of information (*Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften*, ‘TR TKÜV’). While these

Firstly, there is an email-based transmission procedure ('E-Mail-ESB') which is the more basic way of transmitting the information and which any company bound by these obligations has to keep available. Secondly, as a more refined transmission procedure, companies with more than 100.000 customers have to adhere to the transmission procedure through a specific electronic interface ('ETSI-ESB').¹⁶⁶ A transmission by telefax is not allowed.¹⁶⁷ In any way they have to take precautions to ensure that requests as well as disclosures are secure from any changes or from being noticed by third parties,¹⁶⁸ as well as to ensure that any access to these systems is logged according to several parameters.¹⁶⁹ A request may only be processed further after a positive examination of the formal conditions for the request by a responsible professional, if these conditions are not automatically checked by the system.¹⁷⁰

Digital services providers are also required to transmit the data without delay and completely.¹⁷¹ They are required to take into account any source of data internal to the company¹⁷² and to take the arrangements necessary for disclosure at their own expense.¹⁷³ The obligated party has to maintain silence about the request with regard to the concerned party as well as third parties.¹⁷⁴ A request may only be processed further after positive examination of the formal conditions.¹⁷⁵

2.2.5. Sanctions and enforcement mechanisms

OSPs may be subjected to administrative measures and means of compulsion.¹⁷⁶ Persons entitled to refuse to testify are exempt from those measures and means. Those measures and means include: a charge with the costs caused by the refusal;¹⁷⁷ an administrative fine¹⁷⁸ ranging from 5 euros

provisions may directly concern the traffic data request, according to § 31 (7) TKÜV the transmission procedures detailed therein may also be used to transmit subscriber data requests (and consequently also to transmit the subscriber data requested).

¹⁶⁶ Those provisions are detailed in TR TKÜV, pp. 80 ff.; see also Rückert, (n. 129), § 56.

¹⁶⁷ § 174 (7) sentence 4 TKG in conjunction with § 31 (2) sentence 4 TKÜV.

¹⁶⁸ § 174 (7) sentence 4 TKG in conjunction with § 31 (2) sentence 2 TKÜV.

¹⁶⁹ § 174 (7) sentence 4 TKG in conjunction with § 35 TKÜV.

¹⁷⁰ § 174 (7) sentences 5, 6 TKG.

¹⁷¹ § 100j (5) StPO, § 22 (5) sentence 1 TDDDG.

¹⁷² § 22 (1) sentence 4 TDDDG.

¹⁷³ § 22 (6) sentence 1 TDDDG.

¹⁷⁴ § 22 (5) sentence 2 TDDDG.

¹⁷⁵ § 22 (6) sentences 2, 3 TDDDG.

¹⁷⁶ § 100j (5) sentence 2 in conjunction with §§ 95 (2), 70 StPO.

¹⁷⁷ § 70 (1) sentence 1 StPO.

¹⁷⁸ *Ordnungsgeld*, § 70 (1) sentence 2 StPO.

up to 1.000 euros;¹⁷⁹ an arrest order if the fine cannot be recovered¹⁸⁰ ranging from one day to six weeks;¹⁸¹ a detention order to force surrender of the requested object¹⁸² which may not be extended beyond the duration of the proceedings or beyond a period of six months. Any of these measures require a specific court order.¹⁸³ The enforcement requires the person concerned to be aware of their obligation to surrender and of their refusing cooperation on an unlawful basis.¹⁸⁴

2.2.6. Remedies for the concerned person

Considering the general rules protecting the interests of persons concerned by a request and the remedies available to them, this means the following for the subscriber data request in particular: A notification of the person concerned is not necessary for the ‘regular’ subscriber data request, but only for a login data request.¹⁸⁵ A decision of the administrative authority can be contested *via* § 62 OWiG, though due to the absence of a notification the accused will usually not have knowledge of it until they have access to the case file. A court decision, which would also warrant a notification of the accused according to § 35 StPO if their data is being requested, can be contested via a complaint under §§ 304 ff. StPO.

2.2.7. Remedies for the OSP

Regarding the OSPs, their ability to lodge a complaint against a subscriber data request is sometimes categorically denied by the literature.¹⁸⁶ However, others argue that according to § 304 (2) StPO, OSPs are able to lodge a complaint insofar as they can claim a legitimate interest in a court decision.¹⁸⁷ Additionally, it is unclear whether the remedy against administrative decisions set out in § 62 OWiG is available to OSPs requested

¹⁷⁹ Art. 6 (1) of the Introductory Act to the Criminal Code (*Einführungsgesetz zum Strafgesetzbuch*, ‘EGStGB’).

¹⁸⁰ *Ordnungshaft*, § 70 (1) sentence 2 StPO.

¹⁸¹ Art. 6 (2) EGStGB.

¹⁸² *Beugehaft*, § 70 (2) StPO.

¹⁸³ D. Brodowski, ‘StPO § 95’, in: G. Borges, M. Hilber (eds.), *BeckOK IT-Recht*, Munich, Germany, C.H. Beck, 15th ed., 2024, § 16; J. Hauschild, ‘§ 95’, in: C. Knauer, H. Kudlich, H. Schneider (eds.), *MüKo-StPO*, Munich, Germany, C.H. Beck, 2nd ed., 2023, § 18; S. Slawik, ‘§ 70’, in: C. Barthe, J. Gericke (eds.), *KK-StPO*, Munich, Germany, C.H. Beck, 9th ed., 2023 § 15.

¹⁸⁴ Hauschild, (n. 183), § 19.

¹⁸⁵ § 100j (4) StPO.

¹⁸⁶ Greco, (n. 147), § 24.

¹⁸⁷ Rückert, (n. 129), § 73.

to disclose data as well, though reasonably this issue should be handled the same way.

2.2.8. Rules regarding foreign providers, territoriality and concerning conflicting legal obligations

The StPO does not contain any rules specifying the personal scope of the obligations to providers. But since German law requires not only the requesting authority to be competent of the request, but also the requested private actor to be competent to adhere to said request, the corresponding norms of the TKG and of the TDDDG concerning the latter question can be used to determine the scope. According to § 1 (2) TKG, its applicability is not dependent on the location of a telecommunications service's headquarters, but on the location of its services.¹⁸⁸ Therefore, any private actor providing telecommunications services in Germany can be requested according to § 100j StPO. The personal scope of the TDDDG is even wider according to § 1 (3) TDDDG: As an alternative to providing services in Germany, even just maintaining a branch in Germany is enough for it to be applicable.¹⁸⁹

2.3. General requests for information to private third parties

Besides the legal bases aimed specifically at requesting various types of data from OSPs, there are also general norms empowering administrative authorities to oblige private actors to cooperate in the prosecution of regulatory offences by providing information and/or items.

2.3.1. Obligation to surrender (§ 46 OWiG in conjunction with §§ 94, 95 StPO)

§ 95 (1) StPO regulates the obligation of a person to surrender an object they have in their custody. Objects which may be of importance as evidence for the investigation may be requested.¹⁹⁰ It is under debate whether data themselves can be such objects, or whether only a physical object which holds the data can be an object of an obligation to surrender, or whether the obligation to surrender the data themselves is at least permissible, in line with the principle of proportionality, as a less severe alternative to accessing the hardware.¹⁹¹ In practice, § 95 StPO is used as a legal basis for a request of

¹⁸⁸ Cf. also M. Cornils, '§ 1', in: M. Geppert, R. Schütz (eds.), *Beck'scher TKG-Kommentar*, Munich, Germany, C.H. Beck, 5th ed., 2023, § 14.

¹⁸⁹ Cf. also J.-D. Braun, 'TTDSG § 1', in: M. Geppert, R. Schütz (eds.), *Beck'scher TKG-Kommentar*, Munich, Germany, C.H. Beck, 5th ed., 2023, §§ 8 ff.

¹⁹⁰ §§ 95 (1), 94 (1) StPO.

¹⁹¹ W. Wohlers, T. Singelstein, '§ 94', in: J. Wolter, M. Deiters (eds.), *SK-StPO*, Hürth, Germany, Carl Heymanns, 6th ed., 2023, § 27; Brodowski (n. 183), § 6.

data,¹⁹² and the BVerfG has ruled that it is in line with the Constitution that the wording (‘*Gegenstand*’) is extended to non-tangible objects and therefore data as well.¹⁹³ In consequence, § 95 StPO can be used to request any data which may be of importance as evidence for the administrative investigation, as long as it does not fall under any of the following norms, which contain specific safeguards.

First, as for all investigation measures, there needs to be an initial suspicion of a regulatory offence.¹⁹⁴ Also, the requested person must have the requested object in their custody. The majority view is that § 95 (2) StPO implies that objects can also be requested from those entitled to refuse to testify, but there can be no enforcement measures in case of non-compliance.¹⁹⁵ The requested object cannot be subject to a prohibition of seizure under § 97 StPO.¹⁹⁶ Finally, the measure needs to be proportional. In cases where an object is held by multiple persons, surrender may be requested from any of those. However, then any other holder has not given up the object voluntarily, which triggers § 94 (2) StPO calling for a formal surrender and also for their notification.¹⁹⁷ Therefore, when requesting data of an email account, a social media profile or a cloud storage from an OSP, the corresponding user has to be notified.¹⁹⁸ This might also affect cases where a company processes data on behalf of another company, as they might both be regarded as holding the data. If necessary, the ‘controller’ may also be obliged to appeal to the ‘processor’ to submit the data.¹⁹⁹

There are no specific rules for the transfer of data. However, the principle of proportionality may impose specific requirements: If it suffices to surrender a copy of a document, the original cannot be requested; if it is necessary to obtain the original, the holder must be enabled to copy it for themselves.²⁰⁰ If a physical object (for instance, a data storage device) is surrendered, it must be given back when the proceedings are completed.²⁰¹

For the request to surrender an object, it is debated whether a court order is generally necessary – with the exception of exigent circumstances – or

¹⁹² Cf. BGH, decision of 24.11.2009 – StB 48/09, *NJW*, 2010, p. 1297, 1298.

¹⁹³ BVerfG, decision of 16.06.2009 – 2 BvR 902/06, *BVerfGE*, vol. 124, p. 43, 60 f.

¹⁹⁴ § 152 StPO: ‘sufficient factual indications.’

¹⁹⁵ Brodowski, (n. 183), § 11.

¹⁹⁶ *Ibid.*, § 5. This norm prohibits the seizure of correspondence and records of communication between the accused and such persons who are entitled to a right to refuse to testify (as relatives or by their profession, e.g. as their lawyer), if the latter have those objects in their custody.

¹⁹⁷ *Ibid.*, § 9.

¹⁹⁸ *Ibid.*, § 9.

¹⁹⁹ See Hauschild, (n. 183), § 11.

²⁰⁰ Hauschild, (n. 183), § 16.

²⁰¹ J. Hauschild, ‘§ 94’, in: C. Knauer, H. Kudlich, H. Schneider (eds.), *MüKo-StPO*, Munich, Germany, C.H. Beck, 2nd ed., 2023, § 50.

whether such a requirement is to be refused. On the one hand, the StPO explicitly requires a court order only for a seizure, but not for a request and obligation to produce that object. Therefore, it is argued that a court order is not necessary,²⁰² so that the obligation to surrender may be ordered by the investigating authority. On the other hand, it is argued that since the obligation to surrender functions as an alternative to a seizure, which generally requires a court order,²⁰³ this requirement should be extended onto § 95 StPO.²⁰⁴ If one follows the reasoning advocating for the necessity of a court order, the procedure of § 98 StPO would apply. This means that generally a court order would be necessary beforehand. When the delay caused by this procedure would likely lead to a loss of evidence, the investigating authority could order the demand. In this case, the official ordering the demand would have to apply for court confirmation within three days in case the person concerned had issued reservations against the demand.²⁰⁵

2.3.2. General investigative clause (§ 46 (2) OWiG in conjunction with §§ 161, 163 StPO)

The general investigative clause empowers the investigating authority to make investigations of any kind, provided there are no other provisions specifically regulating their powers.

The law²⁰⁶ grants the investigating authority a general right to request any kind of information connected to the investigation²⁰⁷ from all the authorities, who are obligated to comply. While private actors can also be requested to submit information as an informal hearing of a witness based on the general investigative clause ('investigations of any kind'), they are not obliged to comply per se.²⁰⁸ However, in case of non-compliance, they may be subjected to a formal interrogation²⁰⁹ and therefore be obliged to testify truthfully, or to a request to surrender an object and therefore be legally bound to submit said object, or even to a search and seizure.²¹⁰ These potential

²⁰² Hauschild, (n. 183), § 7.

²⁰³ § 98 (1) sentence 1 StPO.

²⁰⁴ Brodowski, (n. 183), § 12.

²⁰⁵ Since the person concerned has to be present in order to fulfil the demand, the necessity of such an application in case of absence is not of interest here.

²⁰⁶ § 161 (1) sentences 1, 2 StPO.

²⁰⁷ Kölbel, Ibold, (n. 107), §§ 23, 1.

²⁰⁸ M. Köhler, '§ 161', in: L. Meyer-Goßner, B. Schmitt (eds.), *StPO*, Munich, Germany, C.H. Beck, 67th ed., 2024, § 2; E. Weßlau, M. Deiters, '§ 161', in: J. Wolter, M. Deiters (eds.), *SK-StPO*, Hürth, Germany, Carl Heymanns, 5th ed., 2016, § 22; M.A. Zöller, '§ 161', in: B. Gercke, D. Temming, M.A. Zöller (eds.), *StPO*, Heidelberg, Germany, C.F. Müller, 7th ed., 2023, § 7.

²⁰⁹ § 163 (3) StPO.

²¹⁰ Köhler, (n. 208), § 2; Zöller, (n. 208), § 7.

consequences may be announced during the initial informal hearing.²¹¹ Thus, the difference to the request from authorities may be seen mainly in the following aspect: Private actors may not be obliged to produce any information, but only to present orally what they actively know or to surrender objects that might hold information by assessment of the prosecution (e.g. documents or hard drives); in contrast, authorities (as well as OSPs based on the special norm discussed in Section 2.2) may be obliged to first gather information from internal sources and present it in written or digital form.

To enable any kind of investigation, there needs to be an initial suspicion of a regulatory offence. There must not be an area-specific obligation of secrecy preventing compliance with the demand; naturally, for authorities the general obligation of official secrecy has no bearing on the duty to fulfil the demand.²¹² Lastly, the measure needs to be proportional. A court decision is not necessary in any case.

3. PUNITIVE ADMINISTRATIVE PROCEEDINGS: SECTORIAL FRAMEWORK

3.1. Requests for data to online service providers

3.1.1. Customs enforcement

Neither the ZollVG nor the ZFdG contain any provisions that empower the customs authorities to request electronic evidence from OSPs for the purpose of administrative punitive investigations. Provisions to request electronic data do exist, namely §§ 10, 30 ZFdG, but their focal point lies on the prevention, mainly of criminal offences. They do not pertain to the prevention or prosecution of regulatory offences. Due to this lack of customs-specific provisions, the general rules as set out in the OWiG apply to requests of electronic evidence from private actors for the purpose of administrative punitive investigations.

3.1.2. Tax enforcement as regards VAT

There is no legal basis specific to the revenue authorities to request evidence from OSPs in investigations of tax-related regulatory offences. However, the law imposes extensive obligations to hand over data for the purpose of facilitating the taxation not only on the taxpayers themselves, but also on third parties. According to § 92 sentence 1 no. 1 AO,²¹³ the revenue

²¹¹ *Ibid.*

²¹² Weßlau, Deiters, (n. 208), §§ 27 ff.

²¹³ The AO is applicable to VAT proceedings (§ 1 (1) sentence 1 AO: ‘all taxes’), but its provisions are modified by the UStG.

authority may gather information from the participants and all kinds of other persons. Specifically, § 93 (1) AO sets out an obligation not only of the (not specifically, but including VAT) taxpayers, but also (secondarily) of other persons to provide the revenue authority with information significant for taxation. The revenue authority may also issue so-called batch information requests according to § 93 (1a) AO about information belonging to as of yet unknown persons.

§ 93 AO is, however, not applicable to the prosecution of tax-related offences,²¹⁴ but only within the taxation procedure. Nevertheless, evidence obtained via such a request might later on be used to prosecute an offence. § 410 (1) no. 4 in conjunction with § 393 AO outline the relation between taxation procedure and prosecution of a tax-related regulatory offence. It is clarified that both procedures are separate. Apart from restrictions relating to data the accused person handed out themselves, evidence acquired via such a request may be used to prosecute a tax-related regulatory offence.²¹⁵

As the OWiG is applicable to all kinds of regulatory offences,²¹⁶ its procedural provisions apply as detailed in Section 2. Due to the substantial range of fines potentially imposed on offenders in some cases potentially concerning also VAT,²¹⁷ a subscriber data request from digital service providers is possible.²¹⁸ For other VAT-related regulatory offences, this is not the case.²¹⁹

3.1.3. Punitive enforcement in the area of banking law and financial markets

There is no legal basis specific to the BaFin to request evidence from OSPs in investigations of regulatory offences related to banking and financial markets. However, similarly to taxation procedure, specific competences to request data exist in relation to the regular administrative supervision procedures in the WpHG as well as the KWG, which are also executed by the BaFin, and also in the BörsG; as an example, § 7 (1) WpHG enables the BaFin to request traffic data from telecommunications services.²²⁰

§ 7 (1) WpHG concerns traffic data – data whose collection, processing and usage is required for the provision of telecommunications services²²¹ –

²¹⁴ H. Kobor, ‘§ 93’, in: V. Pfirrmann, T. Rosenke, J. Wagner (eds.), *BeckOK AO*, Munich, Germany, C.H. Beck, 29th ed., 2024, § 1.

²¹⁵ See § 393 (2) AO.

²¹⁶ § 2 OWiG, cf. also § 410 (1) AO.

²¹⁷ §§ 378 (2), 379 (6), (7), 383 (2) AO.

²¹⁸ Cf. § 46 (4a) OWiG.

²¹⁹ §§ 379 (4), (5), 383b (2) AO.

²²⁰ See also § 7 (2), § 8 WpHG, § 44 (1), § 44c (1) KWG, § 3 (4), (4a) BörsG.

²²¹ § 2 (1) TDDG in conjunction with § 3 no. 70 TKG.

which specifically, but not exclusively,²²² include the following types of data: the number or identifier of the involved ports or terminal equipment, personal authorisation identifiers, card numbers, location data in case of mobile ports; beginning and end of the respective connection according to date and time of day as well as amounts of transmitted data; the telecommunication service utilized by the user; the endpoints of permanent connections, their beginning and end according to date and time of day as well as amounts of transmitted data.²²³ The request is limited to data already existing in possession of the requested company and can therefore not be extended to traffic data of future telecommunication.²²⁴ It targets ‘telecommunications operators’, which is a term not defined within the WpHG. As a result of the unclear terminology, it is disputed in the literature whether the term only includes companies providing telecommunications services commercially²²⁵ or also anyone providing these services noncommercially or only internally.²²⁶ The central condition for such a request is a facts-based suspicion of a breach of specific provisions within the WpHG or specific EU regulations on (financial) market regulation,²²⁷ as well as the necessity of the data to investigate the facts. A court order is required, which is to be applied for by the BaFin.²²⁸

§ 7 (2) WpHG concerns three types of communication data: telephone call recordings, electronic messages as well as the aforementioned traffic data. Just like § 7 (1) WpHG, the request is limited to existing data and linked to several EU regulations.²²⁹ The targeted companies in this case are not OSPs, but several types of companies either requiring licensing or supervision on the basis of these regulations:²³⁰ securities trading companies, data

²²² M. Schramm, I. Shvets, ‘§ 9’, in: S. Assion, *TTDSG*, Baden-Baden, Nomos, Germany, 2022, § 74.

²²³ § 7 (1) sentence 1 WpHG in conjunction with § 9 (1) sentence 1 TDDDG.

²²⁴ M. Hippeli, ‘WpHG § 7’, in: C.H. Seibt, P. Buck-Heeb, R. Harnos (eds.), *BeckOK Wertpapierhandelsrecht*, Munich, Germany, C.H. Beck, 13th ed., 2024, § 13; against this restriction D. Zetzsche, M. Lehmann, ‘WpHG § 7’, in: E. Schwark, D. Zimmer (eds.), *Kapitalmarktrechts-Kommentar*, Munich, Germany, C.H. Beck, 5th ed., 2020, § 21.

²²⁵ Zetzsche, Lehmann, (n. 224), § 9, referencing the now outdated § 2 (3) no. 2 TKG. The same could be concluded now from § 3 (2) sentence 1 TDDDG.

²²⁶ D. Doehmel, ‘WpHG § 121’, in: H.-D. Assmann, U.H. Schneider, P.O. Mülbert (eds.), *Wertpapierhandelsrecht*, Cologne, Germany, Otto Schmidt, 8th ed., 2023, § 8.

²²⁷ Specifically: any provisions of Regulation (EU) No. 600/2014, or Art. 14, 15 of Regulation (EU) No. 596/2014.

²²⁸ § 7 (1) sentence 2 in conjunction with § 100e (1).

²²⁹ Specifically: any provisions of Regulation (EU) No. 600/2014; Regulation (EU) No. 1011/2016; Art. 14, 15 of Regulation (EU) No. 596/2014.

²³⁰ See Zetzsche, Lehmann, (n. 224), § 22.

provision services, credit institutions,²³¹ supervised entities,²³² and financial institutions.²³³

It is important to note that requests based on §§ 6 ff. WpHG, just like those based on special competences within taxation procedure, cannot be made with the goal of prosecuting any regulatory offences. The supervision procedure and the investigation of a connected regulatory offence are separate procedures carried out by separate departments within the BaFin.²³⁴ If supervision and investigation are conducted at the same time, the BaFin has to make clear to which area a specific measure belongs.²³⁵ Data acquired via supervision competences are not admissible in a parallel regulatory offence proceeding.²³⁶

This way of resolving the relationship between preventive and repressive competences can be transferred to the acquisition of data based on § 44 (1) KWG as well as § 3 (4), (4a) BörsG in relation to the prosecution of a corresponding regulatory offence.

Through § 46 OWiG, the provisions of the StPO are applicable. Consequently, the BaFin has the same tools at its disposal as is detailed in Section 2. Due to the substantial range of fines potentially imposed on offenders,²³⁷ a subscriber data request from digital service providers is possible.²³⁸

3.1.4. Competition law enforcement

Pursuant to § 82 (1) in conjunction with § 59 (1) GWB, all information and sources of information that are accessible to the undertaking/association of undertakings or legal entity/association of persons are subject to the request for information.²³⁹ Pursuant to § 82 (1) GWB the ‘Bundesnetzagentur’ (No.

²³¹ Art. 4 (1) no. 1 of Regulation (EU) No. 575/2013.

²³² Art. 3 (1) no. 17 of Regulation (EU) No. 1011/2016.

²³³ Art. 4 (1) no. 26 of Regulation (EU) No. 575/2013.

²³⁴ S. Kämpfer, D. Travers, ‘WpHG § 121’, in: C.H. Seibt, P. Buck-Heeb, R. Harnos (eds.), *BeckOK Wertpapierhandelsrecht*, Munich, Germany, C.H. Beck, 12th ed., 2024, § 7; W. Spoerr, ‘WpHG § 121’, in: H.-D. Assmann, U.H. Schneider, P.O. Mülbert (eds.), *Wertpapierhandelsrecht*, Cologne, Germany, Otto Schmidt, 8th ed., 2023, § 16.

²³⁵ M. Böse, S. Jansen, ‘WpHG § 121’, in: E. Schwark, D. Zimmer (eds.), *Kapitalmarktrechts-Kommentar*, Munich, Germany, C.H. Beck, 5th ed., 2020, § 2; C. Schröder, *Handbuch Kapitalmarktsstrafrecht*, Hürth, Germany, Carl Heymanns, 4th ed., 2020, chapter 5 § 51.

²³⁶ Kämpfer, Travers, (n. 234), § 8; see Chapter 4.3.

²³⁷ §§ 56 (6), 57 (2) sentence 1 KWG, § 120 (17)–(22a) WpHG, § 50 (8)–(10) BörsG.

²³⁸ Cf. § 46 (4a) OWiG.

²³⁹ M. Wirtz, ‘GWB § 59’, in: T. Körber, H. Schweitzer, D. Zimmer (eds.), *Immenga/Mestmäcker Wettbewerbsrecht*, vol 2, Munich, Germany, C.H. Beck, 7th ed., 2024, § 38.

1), the Federal Cartel Office (No. 2 and No. 3) or the Supreme State Authority under state law (No. 3) may be responsible for this. In particular books and business documents in electronic form may be searched as well as data storage locations and passwords.²⁴⁰ The competition authority can also specify the form how to provide the information, especially that the information must be provided in electronic form via an online platform. Moreover, according to § 59b GWB, all items listed in Art. 6 ECN+-Directive²⁴¹ can be subject to a search,²⁴² in particular, therefore, business documents regardless of their form of storage.²⁴³

In *formal administrative proceedings*, the competition authorities may in principle conduct all investigations and collect all evidence that is necessary. Relating to requests for (electronic) evidence from private actors, including OSPs, § 59 GWB gives the competition authority the power to request information from companies, associations of companies, legal entities and associations of persons and contains a power to demand the surrender of documents at the same time. To the extent necessary to fulfil its duties, the competition authority may request the provision of information and in particular the disclosure of documents from companies and associations of companies. The obligation to surrender refers to all (original) documents that are required for the fulfilment of the authority's tasks, regardless of their

²⁴⁰ Cf. § 59b (3) No. 1 and No. 3 GWB; Wirtz, (n. 239), § 20; J. Biermann, 'GWB § 82b', in: T. Körber, H. Schweitzer, D. Zimmer (eds.), *Immenga/Mestmäcker Wettbewerbsrecht*, vol. 2, Munich, Germany, C.H. Beck, 7th ed., 2024, § 15; G. Kallfaß, 'Erweiterte Ermittlungsbefugnisse der Kartellbehörden, §§ 58, 59, 59a und 59b GWB: Behördenperspektive', in: F. Bien, T. Käseberg, G. Klumpe, et al. (eds.), *Die 10. GWB-Novelle – Das neue Kartellrecht*, ch. 2 § 327, Munich, Germany, C.H. Beck, 2021; especially with regard to passwords M. Vetter, 'GWB § 59b', in: W. Jaeger, J. Kokott, P. Pohlmann, et al. (eds.), *Frankfurter Kommentar Kartellrecht*, Cologne, Germany, Otto Schmitt, 108th suppl., 2024, § 22; U. Barth, '§ 59b', in: F.J. Säcker, P. Meier-Beck (eds.), *Münchener Kommentar zum Wettbewerbsrecht (MüKo-Wettbewerbsrecht)*, vol. 2, Munich, Germany, C.H. Beck, 4th ed., 2024, § 18.

²⁴¹ Directive (EU) 2019/1 of the European Parliament and the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market. For example, persons authorised are also empowered to enter any premises, land and means of transport of undertakings and associations of undertakings.

²⁴² § 59b (1) GWB refers to §§ 59 and 59a GWB in a restrictive manner, meaning that only business documents that are requested in accordance with § 59 GWB and that may be inspected and audited in accordance with § 59a GWB may be searched.

²⁴³ Art. 6 (1) lit. b, Directive (EU) 2019/1.

form.²⁴⁴ Provision is also made for transmission in electronic form, in particular via an online platform.²⁴⁵

The investigative powers of §§ 57–59b GWB only relate to formal administrative proceedings and are generally not applicable in the context of administrative *sanctioning proceedings*.²⁴⁶ However, the competition authorities are also granted investigative powers under the general investigative powers of § 46 (1) OWiG in conjunction with the StPO) in sanctioning proceedings. These powers are extended to include the power to request information and the power to demand surrender stated in § 59 (1) GWB as well as the power to ask questions in the context of searches stated in § 59 (3) sentence 1 GWB (in context of § 46 (1) OWiG in conjunction with § 102 StPO).²⁴⁷ The power to request information pursuant to § 82b (1) in conjunction with § 59 (1) sentence 1 GWB extends – as already described above – to information regardless of its form, in particular also stored electronic data. Other investigative powers arise from the general provisions of § 46 (1) OWiG in conjunction with the provisions of the StPO (see above).²⁴⁸

In the following, only the prerequisites for investigative powers in the context of sanctioning proceedings are discussed, § 82b (1) in conjunction with § 59 (1) sentence 1 GWB and § 82b (1) in conjunction with § 59b (3) sentence 1 GWB.

All investigative powers have in common that the competition authority must first have opened an *investigation*. This investigation procedure first requires an *initial suspicion*.²⁴⁹ As in general sanctioning proceedings, it is not permitted to investigate the facts of the case without cause.²⁵⁰ An initial

²⁴⁴ Wirtz, (n. 239), § 64.

²⁴⁵ Cf. § 59 (1) sentence 5 GWB; A. Birnstiel, J.C. Hegener, ‘Verschärfte Ermittlungsbefugnisse deutscher Kartellbehörden – Umfassende Auskunftsverlangen und Mitwirkungspflichten bei Durchsuchungen’ *Der Betrieb*, 2021, p. 1724, 1725.

²⁴⁶ A. Bach, ‘GWB § 54’, in: T. Körber, H. Schweitzer, D. Zimmer (eds.), *Immenga/Mestmäcker Wettbewerbsrecht*, vol. 2, Munich, Germany, C.H. Beck, 7th ed., 2024, § 1.

²⁴⁷ Biermann, (n. 240), § 3, 10; C. Vollmer, ‘§ 82b’, in: F.J. Säcker, P. Meier-Beck (eds.), *MüKo-Wettbewerbsrecht*, vol. 2, Munich, Germany, C.H. Beck, 4th ed., 2024, §§ 24 ff.

²⁴⁸ Cf. Biermann, (n. 240), § 11; G. Kallfaß, ‘Besondere Ermittlungsbefugnisse im Bußgeldverfahren, § 82b GWB’, in: F. Bien, T. Käseberg, G. Klumpe, et al. (eds.), *Die 10. GWB-Novelle – Das neue Kartellrecht*, ch. 3 § 269, Munich, Germany, C.H. Beck, 2021.

²⁴⁹ OLG Düsseldorf, decision of 17.09.2012 – VI-2 Kart 3/12 (V) § 15; Wirtz, (n. 239), § 23; Kallfaß, (n. 240), ch. 2 § 274.

²⁵⁰ Biermann, (n. 240), § 16; Kallfaß, (n. 240), ch. 2 § 274; J.H. Quellmalz, ‘GWB § 59’, in: U. Loewenheim, K.M. Meessen, A. Riesenkampff, et al. (eds.), *Kartellrecht – Kommentar zum Deutschen und Europäischen Recht*, Munich, Germany, C.H. Beck, 4th ed., 2020, § 4.

suspicion exists if the subject of the investigation is a specific set of facts that can justify the application of a substantive provision.²⁵¹

From a formal point of view, the *legal basis*, the *object* and *purpose of the request* for information or disclosure and a *reasonable deadline* must be apparent from the *administrative* act of the competition authority.²⁵² The term ‘information’ is to be understood broadly and includes all factual and legal relationships of the addressee as well as the entire operational and corporate sphere of the company.²⁵³ In addition to sales, products and prices, this may include (in particular) terms and conditions, customers and information on the organisational structure, company agreements and group interrelationships.²⁵⁴ Another key feature is *necessity*.²⁵⁵ Accordingly, the measure is permissible if the authority needs the knowledge to audit the facts of the case or said knowledge will assist it in determining the facts of the case.²⁵⁶ Facts from the past that are irrelevant to the proceedings may not be object of investigations.²⁵⁷ The necessity is only reviewed by the courts to determine whether it was affirmed by the authorities on the basis of justifiable considerations.²⁵⁸ The obligation to disclose and hand over information is limited to such information and business documents that are also accessible to the addressee of the measure.²⁵⁹ Accessibility in turn refers to availability in the economic unit.²⁶⁰ The request for information pursuant to § 82b (1) in conjunction with § 59b (3) sentence 1 no. 1 GWB supplements the general rules on searches in administrative sanctioning proceedings pursuant to § 46 OWiG in conjunction with § 102 ff. StPO. Therefore, the requirements for a general search must be met.

According to § 82b (1) in conjunction with § 59 (1) GWB, there are no rigid time limits. The provision states that the information or disclosure must be provided within a reasonable period of time. In case law, a period of two

²⁵¹ OLG Düsseldorf, decision of 17.09.2012 – VI-2 Kart 3/12; decision of 20.05.2010 – VI-2 Kart 9/09.

²⁵² Wirtz, (n. 239), § 31.

²⁵³ OLG Frankfurt, decision of 12.07.2012 – 11 W 13/12; U. Barth, ‘§ 59’, in: F.J. Säcker, P. Meier-Beck (eds.), *MiKo-Wettbewerbsrecht*, vol. 2, Munich, Germany, C.H. Beck, 4th ed., 2024, § 20; Quellmalz, (n. 250), § 9.

²⁵⁴ Quellmalz, (n. 250), § 9.

²⁵⁵ Vollmer, (n. 247), § 28.

²⁵⁶ OLG Düsseldorf, decision of 04.06.2006 – VI-Kart 6/06 (V), § 27; Vollmer, (n. 247), § 28.

²⁵⁷ OLG Munich, decision of 23.06.1997 – Kart 11/97, guiding principle.

²⁵⁸ OLG Düsseldorf, decision of 17.09.2012 – VI-2 Kart 3/12, § 12; decision of 04.06.2006 – VI-Kart 6/06, § 12; Quellmalz, (n. 250), § 5.

²⁵⁹ Vollmer, (n. 247), § 31.

²⁶⁰ For example, the parent company (e.g. META) is responsible for a request für information if the subsidiary (e.g. Facebook, Instagram, etc.) does not comply with the request for information, cf. Deutscher Bundestag (German Parliament), *Drucksache 19/23492*, 19.10.2020, p. 114; Vollmer, (n. 247), § 31.

to four weeks has so far been considered reasonable.²⁶¹ The public's interest in the swift conduct of proceedings on the one hand and the interests of the addressees (i.e. avoiding an excessive workload) on the other must be weighed against each other.²⁶² Moreover, the competition authority may specify the form of transmission, for example transmission via an online platform § 59 (1) sentence 7 GWB. With regard to § 82b (1) in conjunction with § 59b (3) sentence 1 GWB, no specific deadlines or forms of transmission are specified for this. However, here too, a reasonable period of time (taking into account the proportionality) must be assumed within which the additions must have been communicated.

§ 81 GWB regulates the types of offences, i.e. who is in breach of the regulations in which case. Pursuant to § 81 (2) no. 6 GWB, anyone who intentionally or negligently fails to comply in full or in part with a request for information or surrender contrary to § 59 (2) or (4) GWB (in relation to the sanctioning proceedings also in particular in conjunction with § 82b (1) GWB) shall be deemed to have committed a regulatory offence. Also, anyone who intentionally or negligently fails to comply with a request for information pursuant to § 59b (3) sentence 1 no. 3 GWB, or fails to do so correctly, completely or in time, shall also be deemed to have committed a regulatory offence.

In all of these cases, the sanction is a fine of up to 100.000 euros, § 81c (1) sentence 2 GWB. If an undertaking or an association of undertakings is involved, a fine of up to one percent of the total turnover achieved in the previous year may be imposed for infringements pursuant to § 81 (2) no. 6, 7, 9 and 11 GWB, cf. § 81c (3) GWB. The enforcement of these orders issued by the competition authorities is governed by the provisions applicable to the enforcement of administrative measures, § 86a GWB. With regard to the imposition of penalty payments against undertakings or associations of undertakings, § 86a sentence 2 GWB stipulates that the amount of the penalty payment for each day of delay from the date specified in the warning notice may be up to *five percent* of the average worldwide daily turnover of the company or association of companies in the previous year.

The prosecution of administrative offences by the competition authorities, and thus in particular fines pursuant to §§ 81 ff. GWB, are subject to constitutional guarantees and fundamental rights restrictions. In particular, interventions by the authorities must be weighted against the principle of

²⁶¹ OLG Düsseldorf, judgment of 07.04.2001 – Kart 19/01; OLG Brandenburg, decision of 11.03.2014 – Kart W 1/13; decision of 11.09.2012 – Kart W 2/12.

²⁶² OLG Brandenburg, decision of 11.05.2014 – Kart W 1/13; decision of 11.09.2012 – Kart W 2/12.

proportionality; this applies to both the selection and application of powers.²⁶³ Other principles of constitutional law – as in criminal proceedings – are also applicable in sanctioning proceedings under the GWB. For example, the prohibition of analogy²⁶⁴ and the prohibition of double punishment (*ne bis in idem*)²⁶⁵ under Art. 103 (3) GG should be mentioned.

The legal remedies of persons concerned are generally governed by the provisions of the OWiG (see Section 2). Notably, the person against whom the administrative order imposing the fine is directed may lodge an objection with the cartel authority that issued the administrative order within two weeks in accordance with § 67 OWiG.²⁶⁶

3.1.5. GDPR enforcement

Examining the specific legal basis to request electronic evidence from all private actors – including OSPs –, there are two references in the BDSG, which must be differentiated first. According to § 16 (1) sentence 1 BDSG, the Federal Commissioner shall have the powers referred to in Art. 58 GDPR. Among these figures the right to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks (e) and the right to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law (f). These powers relate to general supervisory and inspection activities, not the prosecution of administrative offences. If the Federal Commissioner concludes that data protection legislation has been violated or that there are other problems with the processing of personal data, they shall inform the supervising authority²⁶⁷ for those specific legal or technical matters.²⁶⁸ Accordingly, the responsibility for the investigation and prosecution of administrative offences does not arise from § 16 BDSG. Therefore, § 41 BDSG has to be considered. Accordingly, investigation and prosecution are largely based on the requirements of the OWiG. The OWiG itself must therefore be consulted and the reference to it must in turn be interpreted:

²⁶³ T. Körber, H. Schweitzer, D. Zimmer, ‘Introduction’, in: T. Körber, H. Schweitzer, D. Zimmer (eds.), *Immenga/Mestmäcker Wettbewerbsrecht*, vol. 2, Munich, Germany, C.H. Beck, 7th ed., 2024, § 4, insofar as there is talk of fundamental rights limits applicable to criminal law.

²⁶⁴ *Ibid.*

²⁶⁵ BGH, decision of 17.12.1970 – KRB 1/70, *GRUR*, 1971, p. 276, 277; BGH, judgment of 24.11.1961 – 2 Str 540/60, *NJW*, 1962, p. 822, 823.

²⁶⁶ Biermann, ‘Preliminary remarks before GWB § 81’, in: T. Körber, H. Schweitzer, D. Zimmer (eds.), *Immenga/Mestmäcker Wettbewerbsrecht*, vol. 2, Munich, Germany, C.H. Beck, 7th ed., 2024, § 306.

²⁶⁷ *Rechts- oder Fachaufsichtsbehörde.*

²⁶⁸ § 16 (1) sentence 2 BDSG.

Unless the BDSG provides otherwise, the provisions of the OWiG and the general laws on criminal procedures, namely the StPO and the GVG, shall apply accordingly in proceedings for violations pursuant to Article 83 (4)–(6) GDPR. The fact that reference is made both to the OWiG and directly to the StPO leaves room for interpretation. If the reference directly to the StPO were prioritised, the restrictions of the OWiG, namely § 46 (3)–(5) OWiG, would not be valid. This is also supported by the fact that the reference to the StPO in other respects is already contained in § 46 OWiG, meaning that the reference in § 41 BDSG would be obsolete. However, such an interpretation would have the consequence that the regulatory offences of the BDSG are *per se* closer to the criminal offences prosecuted by the StPO than those of the OWiG. In addition, the reference to the OWiG would again be obsolete. The better reasons therefore speak in favour of interpreting the reference to the other criminal procedural provisions as merely declaratory.²⁶⁹

The general laws on criminal procedures, namely the OWiG, shall apply accordingly. On the one hand, the reference to the OWiG and indirectly the StPO must be interpreted here, and on the other hand, the deviating choice of words from the reference to § 46 (1) OWiG and § 41 (1) BDSG *mutatis mutandis* must be considered. Moreover, if there is a reference to two different sets of rules – in this case the StPO and the OWiG – it must be clear which one is to be followed in case of doubt. According to one interpretation, the reference in (2) to the StPO and the GVG only has a declaratory effect.²⁷⁰ This view does not address the deviating wording. According to another view, the chosen wording is intended to emphasise a greater parallelism with conventional national sanctioning proceedings.²⁷¹ A third view concludes that the overall view of § 41 (1), (2) BDSG shows that the OWiG should be applied as long as there is no exception.²⁷² Overall, the applicability of § 46

²⁶⁹ VG Stuttgart, judgment of 29.09.2022 – 14 K 5332/20, *BeckRS*, 2022, 38715, § 36; D. Brodowski, D. Nowak ‘§ 41 BDSG’, in: H.A. Wolff, S. Brink (eds.), *BeckOK Datenschutzrecht: DS-GVO, DA, DGA, BDSG. Datenschutz und Datennutzung*, Munich, Germany, C.H. Beck, 48th ed., 2024, § 3; T. Wybitul, J. Zhou, ‘§ 41 BDSG’, in: J. Taeger, D. Gabel (eds.), *DSGVO – BDSG – TTDSG*, Frankfurt am Main, Germany, dfv, 4th ed., 2022, § 19.

²⁷⁰ Wybitul, Zhou, (n. 269), § 19.

²⁷¹ Brodowski, Nowak, (n. 269), § 26; E.M. Frenzel, ‘§ 41 BDSG’, in: B. Paal, D. Pauly (eds.), *Datenschutzgrundverordnung Bundesdatenschutzgesetz*, Munich, Germany, C.H. Beck, 3rd ed., 2021, § 9 calls the choice of word ‘entsprechend’ preferable, but does not address the question of a different interpretation.

²⁷² E. Ehmann, ‘§ 41 BDSG’, in: P. Gola, D. Heckmann (eds.), *Datenschutz-Grundverordnung VO (EU) 2016/679 Bundesdatenschutzgesetz Kommentar*, Munich Germany, C.H. Beck, 3rd ed., 2022, § 11.

OWiG is widely accepted.²⁷³ This means that the exclusions there also apply (see Section 2).

Regarding the restriction of data collection, only the above-mentioned limitations to certain fine amounts need to be addressed again here. The limitation of § 46 (4a) OWiG to fines of a maximum of more than 15.000 euros in relation to natural persons is ‘far exceeded’ by Art. 83 (4)–(6) GDPR.²⁷⁴ In the absence of any mention of data protection offences in the special catalogues of the StPO, none of the other powers of enforcement there come into consideration. At first glance, the principle of proportionality appears to be unproblematically fulfilled with regard to the maximum fines. However, *in praxis* there are also very small fines of between 20 euros and 50 euros, particularly for natural persons, but also for associations.²⁷⁵ Unlike the German catalogue of fines, however, it is difficult to estimate the amount of the fine in advance. So, it is not only the fines that have already been imposed or the associated judgments that provide an indication of the possible amount of the fine. In particular, the catalogue of Art. 83 (1) sentence 2 GDPR should be consulted. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall – for example – be given to the nature, gravity and duration of the infringement taking into account (a), whether there are any relevant previous infringements (e), the degree of cooperation with the supervisory authority (f), and the categories of personal data affected by the infringement (g). Despite the extensive maximum penalties in data protection law, it must therefore be decided on a case-by-case basis whether the respective measures are proportionate.²⁷⁶

3.2. Voluntary cooperation

Voluntary – i.e. not *legally* binding – cooperation with law enforcement authorities occurs in practice in various constellations. Not only so-called confidential counsellors – like the NCMEC – try to collect information proactively in order to pass it on to law enforcement authorities. In practice,

²⁷³ Brodowski, Nowak, (n. 269) § 3; E. Ehmann, (n. 272), § 11; M. Heghmanns, ‘§ 41 BDSG’, in: G. Sydow, N. Marsch (eds.), *DS-GVO/BDSG: Datenschutz-Grundverordnung Bundesdatenschutzgesetz*, Baden-Baden, Germany, Nomos, 3rd ed., 2022, § 23; implicit, as not listed as excluded: M. Bergt, ‘§ 41 BDSG’, in: J. Kühling, B. Buchner (eds.), *DS-GVO BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*, Munich, Germany, C.H. Beck, 4th ed., 2024, §§ 14 ff.; T. Becker, ‘§ 41 BDSG’, in: K.-U. Plath (ed.), *DSGVO/BDSG/TTDSG*, Cologne, Germany, Otto Schmidt, 4th ed., 2023, §§ 3 ff.

²⁷⁴ D. Brodowski, ‘§ 30’, in: A. Klaas, C. Momsen, T. Wybitul (eds.), *Datenschutzsanktionenrecht: Handbuch für die Unternehmens- und Anwaltspraxis*, Munich, Germany, C.H. Beck, 2023, § 31.

²⁷⁵ www.dsgvo-portal.de/gdpr-fine-database/.

²⁷⁶ See in this respect already Brodowski, Nowak, (n. 269) § 22.

‘[i]t is possible and quite common practice for law enforcement authorities to explicitly or implicitly request voluntary information or (the) transmission of digital traces. There is nothing wrong with this in the first instance, *as long as this transmission does not violate the law*.’²⁷⁷

From the perspective of the law enforcement authorities, the question of the legitimacy of the transfer of data to law enforcement authorities primarily concerns the question of the appropriate basis for authorisation, specifically the sufficiency of the general investigation clause. The administrative authority is entitled to request information from all the authorities and to make investigations of any kind, either by itself or through the police authorities and police officers, provided there are no other statutory provisions specifically regulating their powers.²⁷⁸ If a special standard – such as the aforementioned § 100j StPO – is given, its special requirements may not be circumvented. This restricts overly far-reaching powers of intervention, such as preventing the circumvention of a judge’s reservation/court decision requirement or the need for suspicion of an offence.²⁷⁹

It is also necessary to provide the authorisation basis for investigations that do not involve a significant encroachment on fundamental rights and, therefore, do not require any special authorisation to encroach. The general clause authorises the necessary investigative measures that interfere less intensively with the fundamental rights of the citizens.²⁸⁰ In this context, the purchase of so-called tax CDs (data ‘stolen’ from foreign banks pointing to tax evasion), for example, was accepted on the basis of the general investigation clause.²⁸¹

From the perspective of OSPs, the question arises whether and to what extent the transfer of personal data is authorised according to the GDPR, a matter which shall not be discussed in further detail here.

²⁷⁷ M. Jahn, D. Brodowski, ‘Digitale Beweismittel im deutschen Strafprozess – Ermittlungsverfahren, Hauptverhandlung und Revision’, p. 68, 73, in: E. Hoven, H. Kudlich (eds.), *Digitalisierung und Strafverfahren*, Baden-Baden, Germany, Nomos, 2020 [own translation].

²⁷⁸ § 161 (1) StPO (general investigative clause).

²⁷⁹ See, for example, the rejection of the general investigation clause (§ 46 (2) OWiG in conjunction with § 161 (1), sentence 1, § 163 (1), sentence 2 StPO) as the basis for speed or distance measurement by means of video recording regardless of suspicion, discussed in H. Niehaus, ‘Geschwindigkeitsüberwachung durch Videoaufzeichnung – Verfassungsrechtliche Anforderungen und Rechtsfolgen bei fehlender Rechtsgrundlage – zugleich Anmerkung zur Entscheidung des BVerfG vom 11.8.2009 (2 BvR 941/08 2)’ *DAR*, 2009, p. 632, 634.

²⁸⁰ BVerfG, decision of 17.02.2009 – 2 BvR 1372, 1745/07, *NJW*, 2009, p. 1405, 1407 § 26.

²⁸¹ Rhineland-Palatinate Constitutional Court, judgment of 24.02.2014 – VGH B 26/13, *NZWiSt*, 2014, p. 421, 427.

With regard to *competition law* the special regulations §§ 81h–81n GWB regulate the so-called ‘leniency program’. This is intended to help uncover cartels by providing incentives – such as the waiving or reduction of sanctions – to obtain information ‘from within’. The provisions on leniency witnesses pursuant to §§ 81h ff. GWB are applicable to cartel participants, i.e. natural persons involved in cartels as well as companies and associations of undertakings.²⁸² Cartels are defined as agreements or concerted practices between two or more competitors.²⁸³ § 81i GWB contains the requirements for a proper (electronic) application. In particular, pursuant to § 81j GWB, the applicant must disclose their knowledge of and involvement in the cartel to the authority and cooperate fully in clarifying the facts of the case.

§ 81h (3) GWB permits to establish general procedural principles regarding the exercise of its discretion in the application of the leniency program and the structure of the proceedings. The Federal Cartel Office has made use of this with the ‘Guidelines on the Leniency Program’²⁸⁴ of 23.08.2021.²⁸⁵

4. TRANSFER OF DATA BETWEEN PROCEEDINGS

4.1. Transfers of data between national proceedings

In the area of administrative proceedings, the access to data from different proceedings is not governed by one single provision. Instead, the OWiG makes a distinction between an *ex officio* transfer of data on the one hand and the transfer of data in response to a request on the other hand.

The *ex officio* transmission of data allows the courts, public prosecution offices and administrative authorities to transmit personal data from regulatory proceedings to the competent authorities and courts if so required.²⁸⁶ As a prerequisite, the transfer must not happen within the context of the same offence, but from the proceedings pertaining to one offence to the proceedings pertaining to another, separate offence.²⁸⁷ The data transferred is

²⁸² § 81h (1) GWB.

²⁸³ Cf. Art. 2 Abs. 1 Nr. 11 Directive (EU) 2019/1.

²⁸⁴ *Leitlinien zum Kronzeugenprogramm*.

²⁸⁵ Bekanntmachung Nr. 14/2021 über allgemeine Verwaltungsgrundsätze über die Ausübung des Ermessens bei der Gestaltung des Verfahrens und der Anwendung des kartellrechtlichen Kronzeugenprogramms nach §§ 81h–81n GWB. Available at https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Leitlinien/Bekanntmachung_Kronzeugenprogramm_Leitlinien_Oktober2021.pdf?__blob=publicationFile&v=1 (last viewed on 16.12.2024).

²⁸⁶ § 49a OWiG.

²⁸⁷ A. Bücherl, ‘§ 49a’, in: J. Graf (ed.), *BeckOK OWiG*, Munich, Germany, C.H. Beck, 43rd ed. 2024, § 14; J. Lampe, ‘§ 49a’, in: W. Mitsch (ed.), *KK-OWiG*, Munich, Germany, C.H. Beck, 5th ed. 2018, § 13.

personal data as defined by Art. 4 no. 1 GDPR.²⁸⁸ The transmitting agency must deem the data to be required by the competent authorities or courts for one of several specified reasons,²⁸⁹ among them the prosecution of criminal or regulatory offences. The provision does not, however, set out an obligation to transmit data, only a possibility.²⁹⁰ §§ 12 ff. Introductory Act to the Courts Constitution Act ('EGGVG',²⁹¹) concerning general communication obligations are to be applied additionally in cases for which no specific rule can be found in § 49a OWiG.²⁹² For the cases governed by § 49a OWiG, said provision takes precedence.²⁹³

As for the transfer of data in administrative proceedings in response to a request, public prosecution offices and other judicial authorities are as a general rule permitted inspection of the files if this is necessary for the purposes of the administration of justice.²⁹⁴ As with the *ex officio* transfer, this requires two separate proceedings.²⁹⁵ Administrative authorities charged with the prosecution of regulatory offences figure among the 'other judicial authorities' empowered by § 474 (1) StPO.²⁹⁶ The inspection of the files encompasses all the files within the meaning of § 199 (2) sentence 2 StPO,²⁹⁷ i.e. all the files that are available to the court or that would have to be submitted in case of indictment in the proceeding of their origin.²⁹⁸ The included data must have been obtained lawfully.²⁹⁹ Inspection of the files may, as an expression of the principle of proportionality,³⁰⁰ only be granted if it is necessary for the purpose of the administration of justice. It must thus be a necessary, adequate means for the proceedings that encroaches the least on the right of informational self-determination and is proportional to the

²⁸⁸ Bücherl, (n. 287), § 6.

²⁸⁹ § 49a (1) OWiG.

²⁹⁰ Lampe, (n. 287), § 8.

²⁹¹ *Einführungsgesetz zum Gerichtsverfassungsgesetz*.

²⁹² Bücherl, (n. 287), § 20; Lampe, (n. 287), § 17.

²⁹³ Bücherl, (n. 287), § 19; Lampe, (n. 287), § 16.

²⁹⁴ § 474 (1) StPO. According to § 49b OWiG, §§ 474–476, 478–481, 498 (2) StPO are to be applied *mutatis mutandis*, albeit with several changes to adapt these rules to the nature of administrative proceedings.

²⁹⁵ T. Singelstein, '§ 474', in: C. Knauer, H. Kudlich, H. Schneider (eds.), *MüKo-StPO*, Munich, Germany, C.H. Beck, 2019, § 7.

²⁹⁶ Deutscher Bundestag, *Drucksache 14/1484*, 16.08.1999, p. 26; Deutscher Bundestag, *Drucksache 14/9001*, 13.05.2002, p. 13.

²⁹⁷ H. Hilger, '§ 474', in: V. Erb, R. Esser, U. Franke, et al. (eds.), *Löwe-Rosenberg. Die Strafprozeßordnung und das Gerichtsverfassungsgesetz* (LR-StPO), Berlin, Germany, De Gruyter, 26th ed. 2010, § 5.

²⁹⁸ BGH, judgment of 18.06.2009 – 3 StR 89/09, *StV*, 2010, p. 228, 229.

²⁹⁹ P. Wittig, '§ 474', in: J. Graf (ed.), *BeckOK StPO*, Munich, Germany, C.H. Beck, 52nd ed., 2024, § 1.

³⁰⁰ *Ibid.*, § 8; G. Gieg, '§ 474', in: C. Barthe, J. Gericke (eds.), *KK-StPO*, Munich, Germany, C.H. Beck, 9th ed. 2023, § 3.

importance of the proceeding.³⁰¹ It is within the responsibility of the requesting authority to check that these requirements are met.³⁰² Since the provision uses the term ‘are permitted’, the requested authority does not have any discretion when granting inspection of the files, but may deny it in a case of § 479 StPO.³⁰³

As this general rule does not differentiate between criminal proceedings and regulatory proceedings, and is applicable in either case,³⁰⁴ it is also applicable to the transfer of evidence from a criminal to an administrative proceeding. § 49a OWiG explicitly pertains to data from regulatory proceedings and thus does not apply, but so does § 477 StPO in its stead for the *ex officio* transfer.

Considering the transfer of evidence from a criminal to an administrative proceeding, § 49a OWiG governs the *ex officio* transfer of personal data, whilst § 474 StPO, § 49b OWiG cover the requested inspection of the files.

4.2. Transfers of data between foreign and national proceedings

The rules for mutual assistance in criminal matters are laid down in the Act on International Mutual Assistance in Criminal Matters (‘IRG’³⁰⁵), insofar as there are no international agreements (or EU law) which take precedence.³⁰⁶ Its provisions are applicable to regulatory offences as well.³⁰⁷ Special provisions, including for outgoing requests, are laid down in the Guidelines for the Mutual Assistance in Criminal Matters (‘RiVAST’³⁰⁸). The IRG defines ‘criminal matters’ as including proceedings for an offence which is punishable under German law as a regulatory offence by imposition of an administrative fine or which is punishable under the law of a foreign state by imposition of a comparable sanction, provided that a court which also has jurisdiction in criminal matters is able to determine the sanction.³⁰⁹ This means that it makes no difference whether evidence is transferred from a foreign state to a German criminal proceeding or a German administrative proceeding. It also makes no difference whether evidence is transferred from a foreign administrative proceeding or a foreign criminal proceeding,

³⁰¹ Wittig, (n. 299), § 8.

³⁰² OLG Karlsruhe, decision of 21.10.2014 – 2 VAs 10/14, *NStZ*, 2015, p. 606, 608.

³⁰³ Hilger, (n. 297), § 7.

³⁰⁴ §§ 46, 49b OWiG.

³⁰⁵ *Gesetz über die Internationale Rechtshilfe in Strafsachen*.

³⁰⁶ § 1 (3) IRG.

³⁰⁷ § 1 (2) IRG.

³⁰⁸ *Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten*.

³⁰⁹ § 1 (2) IRG.

provided the following conditions are met. In any way, the rules on outgoing mutual assistance requests are applicable.

The rules on outgoing requests are fragmentary.³¹⁰ There are additional requirements for a transfer – relaying as well as receiving – of personal data.³¹¹ Particularly, data may not be used for another purpose than the one for which they were transmitted unless agreed upon by the transmitting authority.³¹² These requirements are modified in case of cooperation with another EU Member State.³¹³ The RiVAST contain specific requirements for a request of surrender of an object that is already in the possession of the requested state.³¹⁴ it stipulates a precise description of the requested object³¹⁵ as well as, if necessary, the attachment of a court order.³¹⁶ Considering this provision, it can be assumed that a court order is generally necessary even if the requested state is already in possession of the object.³¹⁷ On the other hand, there are specific rules on a request of information as well as official documents;³¹⁸ in particular, they always have to go through the foreign judicial authority.

4.3. Admissibility of data collected from online service providers as evidence

In German criminal procedure, the principle of the judge's free evaluation of evidence³¹⁹ determines that the court bases its decision on the result of the taking of evidence at its discretion and conviction based on the entire content of the hearing. Additionally, the court extends the taking of evidence to all facts and means of proof which are relevant to the decision.³²⁰ Hence, any exclusion of evidence is, as an exception to this obligation, to be

³¹⁰ §§ 68 ff. IRG; see T. Hackner, 'IRG vor § 68', in: S. Gleß, T. Hackner, S. Trautmann (eds.), *Internationale Rechtshilfe in Strafsachen*, Munich, Germany, 6th ed., 2020, § 6; D. Brodowski, 'IRG vor § 68', in: C. Kreß, N. Gazeas, D. Brodowski (eds.), *Internationaler Rechtshilfeverkehr in Strafsachen*, Heidelberg, Germany, C.F. Müller, 53rd update to the 3rd ed., 2022, § 1.

³¹¹ §§ 77c ff. IRG.

³¹² § 77h (1) IRG.

³¹³ §§ 97a ff. IRG.

³¹⁴ No. 114 RiVAST, which applies to data as well; M. Fahrner, *Handbuch Internationale Ermittlungen*, Munich, Germany, C.H. Beck, 2020, p. 276.

³¹⁵ No. 114 (1) RiVAST.

³¹⁶ No. 114 (2) RiVAST.

³¹⁷ Fahrner, (n. 314), p. 312.

³¹⁸ No. 118 (2) RiVAST.

³¹⁹ § 261 StPO.

³²⁰ § 244 (2) StPO.

justified.³²¹ Therefore, a violation of law in obtaining evidence only leads to its exclusion if the state's interest in the prosecution of the crime outweighs the interests of the accused person affected by the violation.³²² These principles are applicable in regulatory offence proceedings as well.³²³

The admissibility of data transferred between national proceedings is restricted in some areas. There is a restriction of admissibility of data collected via covert remote search of information technology systems³²⁴ and acoustic surveillance of private premises,³²⁵ which are outside the scope of this report. For the capture of traffic data mandatorily retained,³²⁶ the use in investigations of regulatory offences is barred: The data are only admissible in other proceedings to investigate an offence on the basis of which the measure by which they were collected could hypothetically be ordered.³²⁷ As detailed above, traffic data capture is not applicable to investigate a regulatory offence, so that the transfer of such evidence from a criminal trial is illegal. Another provision extends this principle to all measures of investigation that are bound to the suspicion of particular offences,³²⁸ this applies to regulatory offences procedure as well.³²⁹ In consequence, this means that all data collected from service providers by measures not applicable in regulatory offences procedure for requiring a suspicion of specific offences³³⁰ can also not be transferred to such a proceeding. Considering the intent of this regulation, it should be read as also applying to data collected by such measures which are applicable for all crimes, but not for regulatory offences due to restrictions within the OWiG, TKG and TDDDG.³³¹ Applying this standard to the BaFin's special competence for traffic data requests discussed above,³³² data acquired via such a request cannot be used to prosecute regulatory offences as it is protected by communications secrecy.³³³ For those

³²¹ BVerfG, decision of 07.12.2011 – 2 BvR 2500/09, 1857/10, *BVerfGE*, vol. 130, p. 1, 28; BGH, judgment of 14.08.2009 – 3 StR 552/08, *BGHSt*, vol. 54, p. 69, 87; L. Bartel, '§ 261', in: C. Knauer, H. Kudlich, H. Schneider (eds.), *MüKo-StPO*, Munich, Germany, C.H. Beck, 2nd ed., 2024, § 143. Whether § 261 StPO or § 244 (2) StPO is the primarily relevant norm in this context has no bearing on this question.

³²² BGH, decision of 02.03.2022 – 5 StR 457/21, *BGHSt*, vol. 67, p. 29, 40 f.; Bartel, (n. 321), § 143.

³²³ By way of §§ 46 (1), 77 (1) OWiG.

³²⁴ § 100b StPO.

³²⁵ § 100c StPO.

³²⁶ § 100g (2) StPO.

³²⁷ § 101a (4) StPO.

³²⁸ § 479 (2) sentence 1 in conjunction with § 161 (3) sentence 1 StPO.

³²⁹ § 49a (1) sentence 3, § 49b OWiG.

³³⁰ E.g. § 100k (1), (2) StPO.

³³¹ Especially §§ 100j (2), 100k (3) StPO.

³³² § 7 (1) WpHG; see Section 3.1.3.

³³³ Cf. § 46 (3) sentence 1 OWiG.

measures not restricted to particular offences and therefore applicable to investigate regulatory offences, especially for those measures discussed in detail above, it can be concluded that such data can be freely used in accordance with the exceptions detailed above.

On the admissibility of evidence attained from a foreign country by way of mutual assistance, the Federal Court of Justice ('BGH'³³⁴) has outlined the guiding principles in its decision on 'EncroChat'.³³⁵ The court ruled that the taking of evidence in another state is only to be measured by the law of that state and that evidence transferred into a German proceeding from another state can neither be excluded on the basis of its acquisition violating German nor foreign law.³³⁶ However, the court acknowledged five grounds for exclusion of evidence in such cases:³³⁷

- violations of principles of international law, e.g. a violation of the sovereignty of another state;
- violations of the *ordre public*, especially of fundamental principles regarding the rule of law;
- violations of such provisions of the law of mutual assistance that protect individual rights;
- provisions of the constitution, especially an encroachment on fundamental rights;
- specific provisions in procedural law.

As German criminal procedure law attaches many conditions for the protection of fundamental rights to the taking of evidence rather than the admissibility of evidence, there is a lack of such protection in cases of evidence taken by another state for an investigation of its own and only later transferred to Germany via mutual assistance. In particular, the use of such evidence is not dependent on whether the foreign investigation measure could have been ordered in a domestic case in Germany. Thus, the BGH ruled that there need to be further limitations to the use of that evidence on the basis of fundamental rights, since the taking of the evidence has not been subject to any such restrictions.³³⁸ For this purpose, the provisions restricting data use between domestic proceedings³³⁹ can be applied accordingly.

³³⁴ *Bundesgerichtshof*.

³³⁵ BGH, decision of 02.03.2022 – 5 StR 457/21, *BGHSt*, vol. 67, p. 29, commented by D. Brodowski, 'Anmerkung' *StV*, 2022, p. 364.

³³⁶ BGH, decision of 02.03.2022 – 5 StR 457/21, *BGHSt*, vol. 67, p. 29, 31.

³³⁷ *Ibid.*, p. 33.

³³⁸ *Ibid.*, p. 49 f.

³³⁹ §§ 100c (6), 101a (4), 479 (2), 161 (3) StPO.

5. CONCLUSION

The German rules concerning requests for information from third parties, especially OSPs, within administrative offence proceedings rely predominantly on a general framework regulating the powers of the investigating authorities regardless of the specific sector of administration. The prosecuting authority's competences to request information are derived from those of the public prosecution in criminal matters according to the law of criminal procedure. Still, they are limited: on the one hand, by way of restrictions to the prosecuting authority's powers as laid down in the law of regulatory offences, and on the other hand by way of restrictions to the OSP's authorisation to actually disclose information, as determined by the national laws regulating such providers. While this style of legislation ensures a limitation of prosecutorial powers in line with the principle of proportionality, it does so at the cost of an easily comprehensive regulation. Specifically, the prosecuting authority enjoys the competence to request subscriber data from communications services providers as well as digital services providers. Private actors may also be obligated to surrender any item of significance for the investigation, but they are generally not obliged to disclose information outside of a formal witness hearing. Requests of traffic data or usage data, requests to surrender postal items, as well as any measures interfering with telecommunications secrecy, are off limits. Out of the sectors of administration examined here, only competition law enforcement features any additional competences applicable to investigate regulatory offences. Other sectors, like VAT enforcement as well as banking and financial markets law enforcement, raise the issue of how the much more extensive legal powers that the authorities enjoy within regular administrative procedure can be brought into accordance with their limited competences in prosecution.

8. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN IRELAND

N. NI LOIDEAIN

1. INTRODUCTION

Ireland is the EU base for the headquarters of many national and international online service providers (OSPs).¹ The scope of the term ‘OSP’ used in this chapter is broadly framed. It covers most Internet services, including webmail, messaging providers, hosting providers, domain name registrars, search engines, online gaming services, online marketplaces, financial investment consultants, and other ‘intermediary services’ and ‘information society services’.² There is no consistent definition of the term ‘online service provider’ in Irish law which means that the type of OSP involved will be dependent on the specific statutory regime and relevant sector. ‘Big Tech’ corporations also fall within this scope, serving multiple functions as ‘controllers’, ‘processors’, and ‘third parties’. These OSPs consequently play a pivotal role in the gathering of digital evidence in their provision of data storage and a multitude of other online services to the public and private sectors.³ For such a small country, these factors have understandably led to a consensus among leading scholars that Ireland plays ‘a disproportionately large role’ in the data of the EU and worldwide and the regulation thereof.⁴

¹ All errors are my own. The law is stated as of January 2025.

² On these definitions within EU law, which have also been transposed into Irish domestic law, see Directive (EU) 2015/1535 Internet Society Services (ISS Directive) and Regulation (EU) 2022/2065 Digital Services Act (DSA).

³ On these definitions within the EU legal regime of data protection, see Regulation (EU) 2016/679 (GDPR).

⁴ See, for instance, T.J. McIntyre, ‘Voluntary Disclosure of Data to Law Enforcement’ in: F. Fabbrini, E. Celeste & J. Quinn (eds), *Data Protection Beyond Borders*, p.140, London, United Kingdom, Hart Publishing, 2021; I. Walden, ‘Accessing Data in the Cloud’, p. 466, in: C. Millard (ed.), *Cloud Computing Law*, 2nd ed, Oxford, United Kingdom, Oxford University Press, 2021; G. Giulia and O. Lynskey, ‘Deficient by Design? The Transnational Enforcement of the GDPR’, *International and Comparative Law Quarterly*, 2022, vol. 71, p. 822, DOI:10.1017/S0020589322000355.

Administrative financial sanctions are an established feature in the regulatory toolkits of supervisory authorities of most legal systems in the EU. However, subject to a few exceptions,⁵ Ireland has been a late arrival to this practice.⁶ This gap did not go unnoticed and has in the past led to Ireland being criticised for being ‘out of step’ with its European counterparts, particularly its delay in providing for administrative financial sanctions in its legislation on competition law and data protection law.⁷ Recent changes in enforcement powers in these areas have been (primarily) instigated by a growing wave of EU directives and regulations which provide for the imposition of these sanctions by the relevant competent authorities.⁸ Relatedly, it is essential to note at this juncture that no general legal framework applies to the collection of ‘digital evidence’ in Ireland.⁹

Within this context, this chapter proceeds as follows. Section 2 provides an overview of the general legal framework and requirements applicable to the collection of evidence in administrative proceedings enshrined in Irish Constitutional Law, as applied and developed in the jurisprudence of the Irish courts (common law). Sections 3 and 4 identify relevant national competent authorities that may impose administrative financial sanctions and acquire digital evidence from OSPs in the exercise of their investigatory and enforcement powers. Section 5 deals with the law and practice on the transfer of data as part of these proceedings both nationally and internationally. The chapter concludes with some reflections on the above findings in section 6.

⁵ In 2018, the power to impose administrative financial sanctions was limited to the following legislative regimes: financial services, taxation, regulation of property services, broadcasting, and energy regulation: Law Commission of Ireland, *Report on Regulatory Powers and Corporate Offences*, Vol I, LRC 119-2018, p. 110 (Law Commission Report 2018).

⁶ Significant administrative financial sanctions were recently provided for in the regulatory toolbox of the competition law regulator (CCPC) and the Data Protection Regulator (DPC): Data Protection Act 2018 (GDPR) and Competition (Amendment) Act 2022.

⁷ See Law Commission Report 2018 (n 5) p. 107; European Commission, *Ten Years of Antitrust Enforcement under Regulation 1/2003: Achievements and Future Perspectives*, Communication, COM/2014/0453 final, European Union, 2014.

⁸ Law Commission Report 2018 (n 5) pp. 4, 132-162. On a national level, with a view to reforming the then law, the Law Commission had also recommended that ‘core powers’ in the regulatory toolkit of all ‘financial and economic regulators’ in Ireland should include ‘the power to impose administrative financial sanctions, subject to court oversight, to ensure compliance with constitutional requirements’.

⁹ This applies to both administrative and criminal proceedings in Ireland. On the latter, see T.J. McIntyre & M.H. Murphy, ‘Accessing Digital Evidence in Criminal Matters’: in V. Franssen and S. Tosza (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, pp. 309-346, Cambridge, England, Cambridge University Press, 2025.

2. PUNITIVE ADMINISTRATIVE PROCEEDINGS: A COMMON LAW APPROACH

A growing number of non-judicial bodies are being empowered with statutory powers to issue administrative sanctions Ireland, particularly following a wave of EU law recently enacted and transposed into national law in the past few years that enhance the administrative fine capability of national competent authorities.¹⁰ That said, at the time of writing, most national regulators and competent authorities will more frequently conduct investigations as part of their suite of enforcement powers, rather than conducting punitive administrative proceedings. The domestic legal regime governing the powers of competent authorities to access digital evidence from OSPs for investigations, and to impose any administrative enforcement, is also highly complex due to the lack of codification in Irish law. Instead, the general legal framework for such powers is determined by the statutory and broader governance framework underpinning each specific national competent authority, and the relevant provisions of the Irish Constitution, as interpreted by the Irish courts.¹¹

2.1. The Irish Constitution and the ‘administration of justice’

The primary focus of this judge-made law (or common law) concerns Articles 34 and 37 of the Irish Constitution, regarding the investigating and enforcement powers of national competent authorities in administrative, and criminal, proceedings.¹² Article 34.1 of the Constitution states: ‘Justice shall be administered in courts established by law by judges appointed in the manner provided by this Constitution, and, save in such special and limited cases as may be prescribed by law, shall be administered in public.’ Article 37.1, on the other hand, provides for a ‘saver’ to Article 34.1: ‘Nothing in this Constitution shall operate to invalidate the exercise of limited functions and powers of a judicial nature, in matters other than criminal matters, by any person or body of persons duly authorised by law to exercise such functions and powers, notwithstanding that such person or such body of persons *is not a judge or a court*’.¹³

¹⁰ See F. Keyes, *Administrative financial sanctions*, Spotlight Report, House of the Oireachtas (Irish Parliament), Library and Research Service, Ireland, 2019.

¹¹ On the divergences between civil law and common law systems, see P. Charleton and L. Lochrin, ‘The Mysteries of the Common Law’, *Irish Judicial Studies Journal*, 2023, vol. 7, p. 45; T. Endicott, *Administrative Law*, Oxford, England, Oxford University Press, 5th ed, 2021, pp. 465-546.

¹² On digital evidence access and enforcement in criminal proceedings in Ireland, see McIntyre and Murphy (n 9).

¹³ Emphasis added. Note that the term of ‘saver’ was applied to the interpretation of Article 37 by the Supreme Court (majority verdict) in *Zalewski v. Adjudication Officer* [2021] IESC 24; [2022] 1 IR 421 (O’Donnell J.)

In practice, a competent authority may impose a sanction for a criminal offence, but this will have to be prosecuted *via* the courts (lower or higher) depending on the scale of the penalty (summary or a more serious charge on indictment). Punitive proceedings, for instance, as they relate to competition law enforcement, or pursuant to the GDPR, will involve evidence being gathered by either, or both of, the solicitor involved in the proceedings, or the regulatory competent authority. As such, a barrister/counsel, will not be involved in the collection of the evidence. Evidence gathering in both contexts will be undertaken pursuant to the relevant statutory powers of each authority, and the same approach is adopted to records that are either digital or traditional (paper-based) evidence. However, there are some safeguards regarding electronic evidence following the jurisprudence of the Irish courts, to the effect that seizure of electronic evidence from the party holding such material (an OSP) cannot be in a blanket form. The related search and collection of evidence must also subject to the rule of law, and satisfy the requirements of proportionality, as provided in ‘the protections of the [Irish] Constitution and Article 8 ECHR.’¹⁴

The most significant case on the administration of justice by a non-judicial body and administrative proceedings was delivered by the Irish Supreme Court in the case of *Zalewski v. Adjudication Officer*.¹⁵ The Supreme Court (by a 4-3 majority) rejected a legal challenge contesting the constitutionality of the State’s system for resolving workplace disputes, and raised questions about the constitutionality of the administration of justice by administrative bodies more broadly. Ultimately, the Court held that the power of an administrative body, in this case the Workplace Relations Commission (WRC), to adjudicate disputes between employers and staff fell within Article 37 of the Irish Constitution. The Supreme Court reached this assessment on the main ground that the WRC was exercising ‘limited powers and functions of a judicial nature’ which therefore did ‘not offend the Constitution’.¹⁶

¹⁴ See Irish Supreme Court case of *RH Plc, Irish Cement Ltd v Competition and Consumer Protection Commission* [2017] IESC 34. On recent literature and ECtHR case law concerning Article 8 ECHR protections provided to legal entities and third parties, such as OSPs, see ECtHR, *Ships Waste Oil Collector BV and Others v the Netherlands*, 01.04.2025, no. 2799/16; N. Ni Loideain, *EU Data Privacy Law and Serious Crime*, Oxford, England, Oxford University Press, 2025.

¹⁵ [2021] IESC 24. O’Donnell J. delivered the majority judgment (4-3) of the Supreme Court. Note the strongly dissenting judgment of MacMenamin J. See other judgments by McKechnie J. and Charleton J. On the case generally, including the High Court judgment, see T. Hickey, ‘*Zalewski* and the Future of Irish Public Law’, *Modern Law Review*, 2024, vol. 87, pp. 446-483, DOI:10.1111/1468-2230.12847.

¹⁶ [2021] IESC 24 § 117 (majority judgment).

2.2. *Zalewski*: ‘fair procedures’ for investigated persons and administrative sanctions

Consequently, as established in *Zalewski*, bodies other than the courts in Ireland may exercise limited functions and powers of a judicial nature in matters other than criminal matters (Article 37 of the Constitution of Ireland). The Irish Supreme Court emphasised that such powers are exercised as part of the ‘administration of justice’ by quasi-judicial bodies. In doing so, the Court made clear that such competent authorities when performing this function, and exercising such powers, ‘must comply with the fundamental components of independence, impartiality, dispassionate application of the law, openness, and, above all, fairness, which are understood to be the essence of the administration of justice.’¹⁷ In addition, the Court made clear that the law and the principles of fair procedures applied by such bodies must be to a high standard: ‘[t]he standard of justice administered under Article 37 cannot be lower or less demanding than the justice administered in courts under Article 34.’¹⁸

This high standard set by the Supreme Court in *Zalewski* has significant implications for administrative bodies and the exercise of their powers, including administrative financial sanctions. Administrative agencies (non-judicial bodies) are thus required not just to adhere to fair procedures but may be conducting the administration of justice depending on the nature of their role. The latter of which therefore brings into play judicial type obligations, such as the need for a public hearing.¹⁹ Thus, the ‘blanket prohibition’ on public hearings before an adjudication officer in the contested employment legislation in *Zalewski* (Workplace Relations Act 2015) (Act of 2015) was criticised for its incompatibility with Article 34.1 on the grounds *inter alia* that a public hearing is ‘fundamental to the administration of justice, and as establishing a principle from which any exception must be justified.’ The ‘absolute ban’ in this case had not been shown as justified to the Supreme Court.²⁰ Omission of this established constitutional law safeguard in the impugned legislation was particularly striking as the Irish legislator ‘commonly provides for a statutory right of appeal from certain decisions of adjudicative bodies’.²¹

¹⁷ [2021] IESC 24 § 138 (majority judgment).

¹⁸ [2021] IESC 24 § 138 (majority judgment).

¹⁹ [2021] IESC 24 § 142 (majority judgment).

²⁰ [2021] IESC 24 §§ 142-143 (majority judgment). As held by O’Donnell J.: ‘Article 34.1 of the Constitution makes clear that public hearings are of the essence of the administration of justice’. Note that all seven judges were satisfied that the blanket ban on a public hearing was unconstitutional.

²¹ Law Commission Report 2018 (n 6) p. 145.

Secondly, and relatedly, the Court held ‘the absence of at least a capacity to allow the adjudication officer to require that certain evidence be given on oath [to be] inconsistent with the Constitution.’²² Thirdly, the legislation was criticised for not including any express provisions for the cross-examination of witnesses. Fourthly, this was found to be problematic ‘particularly when the Act is meant to be capable of being operated by persons *without any knowledge of the law*’ and for decisions to be made by persons ‘without any broader legal experience or training’.²³ The Court refrained, however, from concluding that the legislation was rendered unconstitutional as a result of the lack of this express reference as the non-statutory guidelines ‘expressly referred to the right to question and cross-examine witnesses.’²⁴ Finally, the Irish Supreme Court turned to the issue of the independence of decision-makers and observed that ‘independence’ and ‘impartiality’ are ‘fundamental components of the capacity to administer justice.’²⁵

The Irish Supreme Court as a result criticised a ‘troubling’ provision in the contested legislation which allowed for a Minister of the government to have an ‘unqualified power of revocation of appointment’ of an adjudication officer appointed under the Act of 2015. Although this matter did not fall within the main arguments of the case, the Court nevertheless stressed that it now requires ‘at a minimum ... careful scrutiny in the light of the conclusion of this Court that the functions being performed are functions of a judicial nature involving the administration of justice under the Constitution.’²⁶ In addition, the Court stressed that these considerations are not peculiar to the Irish constitutional order. The guarantees of impartiality and independence are also ‘essential requirements for any adjudication’ within the scope of EU law, Article 6 ECHR and the jurisprudence of the European Court of Human Rights.²⁷

Zalewski represents a landmark development for Irish public law and has set standards with far-reaching implications for administrative sanctions issued by non-judicial bodies. The majority judgment of the Supreme Court (4-3) marks a clear shift away from the traditional approach established in the 1965 case of *McDonald v Bord na gCon (McDonald)*. A leading judgment which had identified five elements a judge would previously have considered in assessing whether a process had the ‘characteristic features’ of the administration of justice.²⁸ The previous five-point test, as set out in *McDonald* for what constituted an administration of justice under Article 34.1

²² [2021] IESC 24 § 145 (majority judgment).

²³ [2021] IESC 24 § 146 (majority judgment).

²⁴ [2021] IESC 24 § 146 (majority judgment).

²⁵ [2021] IESC 24 § 147 (majority judgment).

²⁶ [2021] IESC 24 § 147 (majority judgment).

²⁷ [2021] IESC 24 § 147 (majority judgment).

²⁸ *McDonald v Bord na gCon* [1965] IR 217.

required the existence of the following: ‘1) a dispute or controversy as to the existence of legal rights or a violation of the law; 2) the determination or ascertainment of the rights of parties or the imposition of liabilities or the infliction of a penalty; 3) the final determination (subject to appeal) of legal rights or liabilities or the imposition of penalties; 4) the enforcement of those rights or liabilities or the imposition of a penalty by the court or by the executive power of the State which is called in by the court to enforce its judgment; and 5) the making of an order by the court which, as a matter of history, is an order characteristic of courts in this country.’²⁹

Instead, as Hickey highlights, the majority judgment in *Zalewski* has established ‘a more impressionistic/normative approach under which a judge would assess whether the process, considered in the round, was one which ought to be carried out by an Article 34 court.’³⁰ In addition, the Court held that law and the principles of fair procedures applied by such bodies must be to a high standard the standard of justice administered under Article 37 ‘cannot be lower or less demanding’ than the justice administered in courts under Article 34. Administrative agencies are thus required not just to adhere to fair procedures but may be conducting the administration of justice depending on the nature of their role. The latter of which therefore, as noted above, brings into play judicial type obligations. The standards set in *Zalewski* have already influenced reforms in various sectors. This includes investigatory and enforcement powers within the regimes of Irish Competition Law and Banking and the Financial Markets, as evident in the Competition (Amendment) Act 2022 and Central Bank (Individual Accountability Framework) Act 2023.

2.3. *Zalewski*: implications for OSPs as third parties in administrative proceedings

Irish judges have long tended to ‘jealously guard’ the judicial power as enshrined in Article 34.1 of the Irish Constitution as the sole remit of the courts and have consequently determined what constitutes ‘fair procedure’ within a non-judicial body – ‘not the non-judicial actors operating at the coalface’.³¹ *Zalewski*, as Hickey and others argue, indicates a shift away from the rigid judicial ‘centralism’.³² That said, when one considers how *Zalewski*

²⁹ [1965] IR 217, p. 231 (Kenny J.). As reiterated in *Zalewski v Adjudication Officer* [2021] IESC 24 (majority judgment) § 16.

³⁰ Hickey (n 15) p. 468.

³¹ *Ibid*, p. 446. See further P. Daly, ‘The Irish Courts and the Administrative State’, pp. 264-266., in: D.M. Farrell and N. Hardiman (eds.), *The Oxford Handbook of Irish Politics*, Oxford, England, Oxford University Press, 2021.

³² *Ibid*.

‘split the Irish Supreme Court’,³³ it would be remiss not to consider the argument that Irish constitutional law still provides that ‘it is clear that Article 34.1 is to be interpreted in a manner protective of the jurisdiction of the courts.’³⁴ Consider, for instance, the reasoning of Charleton J. in his dissent: ‘[i]n a complex modern environment where rights are often created by statute and administered by specialised bodies, it does not infringe the Constitution for these to be considered by non-judicial figures. Where, however ... those rights transcend what is limited or technical, but go to the *very core of what defines a person in their social standing or conduct*, there must be a choice ... to seek justice in a court by way of a final factual appeal that requires a rehearing.’³⁵ Any future challenges to the powers of non-judicial bodies to issue significant administrative financial sanctions to an OSP, for their non-compliance (as a controller, processor, or third party) in their provision of digital evidence as part of an investigation, would thus likely be closely scrutinised by the Irish courts. Specifically, whether the proportionality of any fines would fall within the realm of ‘criminal matters’ rather than administrative, thereby placing the exercise of such powers beyond the ‘limited’ scope accorded to non-judicial bodies by Article 37 of the Constitution.

3. COMPETENT AUTHORITIES IN SELECTED AREAS OF PUNITIVE ADMINISTRATIVE ENFORCEMENT

3.1. Digital Regulators Group (DRG)

The following bodies comprise the ‘Digital Regulators Group’ (DRG): Commission for Communications Regulation (ComReg), Competition and Consumer Protection Commission (CCPC), Data Protection Commissioner (DPC), and the Media Commission (Coimisiún na Meán). This term was coined by the Irish Government in 2022 as part of its policy strategy for Ireland to be ‘a European and global digital leader’.³⁶ Only those competent authorities that fall within the scope of the ELEVADMIN Project and have investigatory powers to acquire digital evidence from OSPs in punitive administrative enforcement proceedings are discussed. They are primarily tasked with monitoring, individually and jointly, the compliance by OSPs in

³³ Hickey (n 15) p. 479.

³⁴ P. Daly, ‘The Administration of Justice in Administrative Tribunals’, *Administrative Law Matters*, 2023, online <https://www.administrativelawmatters.com/blog/2023/10/17/the-administration-of-justice-in-administrative-tribunals-zalewski-v-adjudication-office-2021-iesc-24-article-34-1/>.

³⁵ Judgment of Charleton J. in *Zalewski* (n 14) § 71 (emphasis added).

³⁶ Government of Ireland, *Harnessing Digital: The Digital Ireland Framework, 2023 Progress Report*, 2024.

specific (and at times overlapping) areas of digital regulation, such as data protection.³⁷ All authorities within the DRG have administrative fine capability but there are differences in how they may exercise their investigatory powers when it comes the collection of digital evidence from OSPs as third parties in punitive administrative proceedings.

3.1.1. Competition and Consumer Protection Commission (CCPC)

The nature of the enforcement powers of CCPC is administrative and criminal.³⁸ As is the case in other European jurisdictions, the CCPC is the national regulator tasked with enforcing both competition and consumer protection rules.³⁹

3.1.2. Data Protection Commissioner (DPC)

The nature of the DPC's enforcement powers is administrative and criminal.⁴⁰ The DPC is tasked as part of its role as the supervisory authority for monitoring compliance with data protection law and with investigating and issuing punitive administrative sanctions to OSPs. This includes the power to access electronic evidence as part of these proceedings. These investigative and corrective powers were granted to the DPC following the transposition of EU GDPR into Irish law *via* the Data Protection Act 2018.⁴¹ Most enforcement proceedings undertaken by the DPC concern its administrative powers. The importance of compliance with data protection law in relation to competition law enforcement across the EU has become more concretely linked since the judgment of the CJEU in the *Meta Platforms* case which determined that a breach of the GDPR may be investigated by a

³⁷ Two Irish regulators within the DRG (Media Commission & CCPC) are tasked with the responsibility of monitoring compliance and enforcement of different obligations for OSPs concerning online harms under the EU Digital Services Act (DSA). Other authorities, such as the Commission for Communications Regulation (ComReg) and the DPC, may share information with each other.

³⁸ See, for instance, the significant sanctions under section 9 of the Competition (Amendment) Act 2022 which provide for a breach of certain anti-competitive practices under Article 81 of the Treaty of the EU - based on a conviction on indictment - that an individual may be subject to both a fine of 50,000,000 EUR and a term of imprisonment of up to 10 years.

³⁹ These include Italy, the Netherlands, the United Kingdom, and Poland.

⁴⁰ The Data Protection Act 2018 which transposed the GDPR into Irish law also brought over the limited criminal offences that the DPC may enforce as provided under the e-Privacy Directive 2002/58/EC.

⁴¹ See Article 58 GDPR on the granting to data protection authorities (DPAs) of investigatory powers, and corrective powers, including the imposition of administrative fines (subject to the requirements in Article 83).

national competition authority and lead to a breach of competition law.⁴² In practice, within the sphere of banking and finance, regulatory breaches tend to be dealt with by the Central Bank of Ireland (CBI), rather than the DPC.⁴³

3.2. Other competent authorities

3.2.1. Central Bank of Ireland (CBI) (Banking and Financial Services)

The nature of the CBI's enforcement powers is administrative and criminal.⁴⁴ Its responsibilities primarily concern ensuring monetary and financial stability, but its enforcement responsibilities also extend to other sectors (such as consumer protection).⁴⁵ Its enforcement work relies principally on two processes.⁴⁶ One is the statutory requirement that individuals in designated positions within regulated firms meet the standards of 'fitness and probity' ('Fitness and Probity Routine').⁴⁷ The second, and most relevant to this chapter, concerns how the CBI investigates and sanctions breaches of financial services law by regulated firms and individuals ('Administrative Sanctions Procedure') (ASP).⁴⁸ The scope of the investigative powers of the CBI depends on the process that is being followed. Where an ASP is concerned, the Central Bank at the investigation stage will gather information through its investigative powers, which include compelling the production of (electronic) documents and conducting onsite

⁴² ECJ, *Meta Platforms v Bundeskartellamt*, 04.07.2023, C-252/21.

⁴³ Such an approach recognises the 'duty of sincere cooperation' between regulators, as set out by the CJEU (sitting as the Grand Chamber) in *Meta Platforms*.

⁴⁴ The Central Bank may, for instance, prosecute and direct the courts to impose a fine on an individual who commits an offence of false disclosure of information as part of a review investigating 'the proper and effective regulation' of a financial service provider of up to €5,000 ('Class A Fine') or imprisonment for 12 months or both (on summary conviction) or a fine up to €250,000 or imprisonment for 5 years or both (on indictment). See section 18, Central Bank (Supervision and Enforcement) Act 2013 (as amended).

⁴⁵ For instance, the Central Bank in 2020 was made the designated competent authority for enforcement of certain consumer protection issues (including unfair commercial practices, consumer financial services). See S.I. No 14/2020 – EU (Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws) Regulations 2020.

⁴⁶ The Central Bank also cooperates with other agencies. For instance, it is obliged to report to the police (An Garda Síochána) and others, such as, the Office of the Revenue Commissioners, where there is evidence that a criminal offence may have been committed.

⁴⁷ Section 21, Central Bank Reform Act 2010.

⁴⁸ See the Central Bank, ASP Guidelines (last updated December 2023).

inspections.⁴⁹ In practice, any gathering of evidence from a third party to an investigation (such as from an OSP) will be done on a voluntary basis.

The ASP enforcement powers of the CBI were significantly expanded under the Central Bank (Individual Accountability Framework) Act 2023. Regarding the gathering of digital evidence from OSPs, the Act of 2023 introduces the role of ‘a responsible authorised officer’ within the Central Bank who will be responsible for any ASP investigations. This role includes the acquiring of evidence from any third parties (including OSPs) involved in an ASP investigation. Administrative sanctions can be imposed under Part IIIC of the Central Bank Act 1942 (as amended), and separately under the Securities and Markets Regulations.⁵⁰ In terms of enforcement powers, different sanctions are available depending on the process followed. Under the ASP, sanctions for regulated firms include: a caution or reprimand; suspension or revocation of authorization, and/or fine of up to 10 million EUR or 10% of the firm’s national turnover.⁵¹ An individual may be subject to a caution or reprimand; disqualification from managing a regulated firm for a specified period, and/or a fine of up to one million EUR.⁵²

3.2.2. Office of the Revenue Commissioners (VAT Enforcement)

The nature of the Revenue Commissioners’ enforcement powers is administrative and criminal.⁵³ The Revenue Office was established in 1923 by Government Order, and it is the primary State body primarily responsible for the assessment and collection of taxes and duties and implementation of customs rules. This includes administering the customs regime for the control of imports and exports and collection of duties and levies on behalf of the EU, and co-operation with other State agencies in the fight against drugs, and

⁴⁹ Central Bank Act 1942, as amended by the Central Bank (Supervision and Enforcement) Act 2013, and the Central Bank (Individual Accountability Framework) Act 2023.

⁵⁰ See Regulation 41, EU (Market Abuse) Regulations 2016; Regulation 99, Prospectus (Directive 2003/71/EC) Regulations 2005, as amended; Regulation 67, Transparency (Directive 2004/109/EC) Regulations 2007, as amended; Regulation 32, European Union (European Markets Infrastructure) Regulations 2014. These are collectively referred to as the ‘Securities Markets Regulations’.

⁵¹ Central Bank, ASP Guidelines (December 2023).

⁵² Section 33AQ(4) of Central Bank Act 1942, as amended by section 68 the Central Bank (Supervision and Enforcement) Act 2013. See Central Bank, Outline of the Administrative Sanction Procedure (2018), § 6.2.1.

⁵³ The Revenue Office is split into 16 divisions. Different divisions are responsible for administrative and criminal enforcement actions. The Collector General’s Division is responsible for taking administrative enforcement action for non-compliance.

other cross-departmental policies.⁵⁴ Its broad mandate derives from Irish law and EU law. Any assets arising from criminal activity, such as drug trade, are investigated by another competent authority, the Criminal Assets Bureau (CAB).⁵⁵

4. PUNITIVE ADMINISTRATIVE PROCEEDINGS: SECTORAL APPROACHES

4.1. Requests for data: voluntary cooperation from OSPs by default

The main way in which administrative enforcement authorities in Ireland acquire electronic evidence from OSPs is by request from the relevant OSP who provides this information on a voluntary basis.⁵⁶ In most instances, companies (including as third parties) will also tend to cooperate with any regulators who make a request for data. That said, if they are concerned about what is being requested, or the scope of what is being requested, they will seek legal advice from counsel (a barrister) and then respond to the request accordingly. The scope of the data provided may then be limited subject to the advice provided by counsel regarding the proportionality of the request, and other considerations (such as trade secrets, client confidentiality). Although some have argued for a stricter approach,⁵⁷ it is rare in practice for competent authorities in Ireland to have to issue ‘an information notice’ to access any digital evidence from an OSP (as a controller or processor).⁵⁸

For instance, section 132(1) of the Data Protection Act 2018 states: ‘The Commission or an authorised officer may, by notice in writing ... served *on a controller or processor*, require the controller or processor to furnish, in writing, within such period as may be specified in the notice and, if applicable, in the format or manner specified in the notice, such information in relation to matters specified in the notice as is necessary or expedient’.⁵⁹ Note, however, that this notice from the DPC does not extend to OSPs if their

⁵⁴ The Revenue Office has published detailed and specific guidance on the application of administrative penalties for infringements of custom rules. Regulation of the customs rules is not explored here as it falls outside the scope of the ELEVADMIN Project. For further, see (updated April 2024).

⁵⁵ Revenue co-operates in this work through the disclosure of relevant information with CAB and co-operation with other. Customs enforcement within the context criminal proceedings, such as money laundering, falls outside the remit of the ELEVADMIN Project.

⁵⁶ On the voluntary cooperation of OSPs in providing electronic evidence within the context of criminal proceedings, see McIntyre and Murphy (n 9).

⁵⁷ Law Commission Report 2018 (n 6) p. 4. The Law Commission of Ireland previously advocated that ‘core powers’ in the regulatory toolkit of ‘financial and economic regulators’ should include ‘the power to require persons to attend in person before the regulator, or an authorised officer, to give evidence or *to produce documents*’. Emphasis added.

⁵⁸ See a relevant legislative power to do so for VAT Enforcement below.

⁵⁹ Emphasis added.

role in holding this information is as a ‘third party’ (such as Amazon, a third party data storage hosting service). This gap, of course, is consequently not an issue for competent authorities under the voluntary cooperation regime which contains no such limitations. Despite the practice not being legally binding, this mechanism has (yet) to present itself as an evidential challenge for competent authorities acquiring electronic information from OSPs.⁶⁰

4.2. Enforcement by Digital Regulators Group (DRG)

The competent authorities that comprise the DRG are primarily tasked with monitoring and enforcing compliance by OSPs in specific (and at times overlapping) areas of digital regulation, such as data protection and online content moderation. The second group includes other national authorities with administrative powers of investigation and enforcement in distinct areas of competence, such as employment law, which are also relevant to the regulation of OSPs with establishments in Ireland.

4.2.1. GDPR enforcement

The scale of administrative fines permitted under the GDPR represented a significant reform to the data protection enforcement powers of the DPC.⁶¹ Previously, the DPC may have brought criminal proceedings before the courts against individuals, or companies, but any convictions were subject to far less significant fines. For instance, under the e-Privacy Regulations 2011,⁶² a company providing a publicly available electronic communications network or service, found by the DPC not to have undertaken appropriate technical and organisational measures to safeguard the security of its services, if convicted on indictment by the Circuit Court, may be subject to a fine of up to a maximum of 250.000 EUR.⁶³

⁶⁰ On the legal and procedural precarity and risk to fundamental rights posed by heavy reliance on this voluntary mechanism, see S. Tosza, ‘Internet service providers as law enforcers and adjudicators’ (2021) 43 *Computer Law & Security Review* 1-17.

⁶¹ Article 83(5) GDPR permits DPCs to issue administrative fines of up to 4% of worldwide annual turnover for the preceding financial year. It is notable that public authorities in Ireland are exempt from these larger fines, with a limit of up to 1 million EUR that may be imposed by the DPC and then confirmed by the Circuit Court. See section 141(4), Data Protection Act 2018.

⁶² In addition to the GDPR, the DPC is responsible for monitoring compliance with other related data protection instruments. These include the Irish e-Privacy Regulations 2011 (e-Privacy Directive 2002/58/EC, as amended by Directive 2009/136/EC) and the Law Enforcement Directive (EU) 2016/680. The 2011 Regulations transposed the e-Privacy Directive 2002/58/EC into Irish law.

⁶³ Regulation 4(14), European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. No 336/2011).

2023 was an unprecedented year for the DPC regarding the exercise of its administrative fine powers concerning OSPs under the GDPR. The DPC issued 19 finalised decisions resulting in administrative fines totalling 1.55 billion EUR, the three largest of which concerned foreign OSPs.⁶⁴ As the DPC is the ‘Lead Supervisory Authority’ as defined in the GDPR in cases where a company has its sole, or main establishment, in the EU, the DPC led both investigations.⁶⁵ In 2023, the DPC issued 87% of all GDPR enforcement fines across the EU.⁶⁶ This gives and places, as Lynskey and Gentile aptly highlight, an ‘outsized’ role and burden on the Irish supervisory authority when it comes to the cross-border enforcement of the GDPR.⁶⁷ Consequently, the path to reaching these significant cross-border decisions were highly complex, difficult, and remain the subject of legal uncertainty. Indeed, the legal certainty and effectiveness of these unprecedented administrative fines are still open to question with all three final decisions under appeal before the High Court in Ireland.⁶⁸ Although the OSPs in these cases are the investigated parties, these post-*Zalewski* appeals could have far-reaching implications for any future administrative financial sanctions the DPC could bring against OSPs as third parties that do not comply with information requests relevant to investigations undertaken by the DPC (or other non-judicial bodies).

4.2.2. Competition law enforcement

As is the case in other European jurisdictions, the CCPC is the national regulator tasked with enforcing both competition and consumer protection rules.⁶⁹ Graef and others suggest that this model of both regimes being enforced by one competent authority implies that the relevant expertise is present to rely on ‘consumer protection principles’ in order to establish a violation of competition law in cases where this is desirable to enhance the ‘effectiveness of the competition regime’.⁷⁰ Under the Competition (Amendment) Act 2022 (Act of 2022),⁷¹ the CCPC gained new and expanded powers including new powers to issue significant administrative fines. The

⁶⁴ Data Protection Commission, *Annual Report 2023*, May 2024, pp. 31-32.

⁶⁵ Article 56 GDPR.

⁶⁶ DPC, *Annual Report 2023*, 4.

⁶⁷ Note that Luxembourg also plays a disproportionate role compared to other EU Member States in cross-border proceedings within the sphere of EU GDPR enforcement: O Lynskey and G Gentile, ‘Deficient by Design? The Transnational Enforcement of the GDPR’ (2022) 71 *International and Comparative Law Quarterly* 799, 800, 822.

⁶⁸ DPC, *Annual Report 2023*, 38-39. At the time of writing, these court proceedings remained ongoing.

⁶⁹ These include Italy, the Netherlands, the United Kingdom, and Poland.

⁷⁰ I Graef, D Clifford, and P Valcke, ‘Fairness and Enforcement: bridging competition, data protection, and consumer law’ (2018) 8 *International Data Privacy Law* 200, 213.

⁷¹ Competition (Amendment) Act 2022 (came into force in September 2023).

Act of 2022, the principal aim which was to implement the ECN+ Directive, brought the CCPC in line with the investigative and enforcement powers of its EU competition law counterparts.⁷² Most enforcement proceedings undertaken by the CCPC concern its administrative powers.

There is no specific legal basis to request electronic evidence from OSPs. However, section 18 of the Act of 2022 provides a power to require the production of evidence which includes ‘any books, documents and records in his or her power or control.’ Documents in Irish law are defined as including electronic records, and documents. Any OSP would fall within this scope if subject to a complaint under Articles 101/102 TFEU, or pursuant to national consumer protection or competition measures.⁷³ Penalties may be imposed by the CCPC on an OSP that does not comply with a request for digital evidence. Since the commencement of the Act of 2022, the CCPC can impose fines of up to 10 million EUR, or 10% of annual turnover, whichever is greater.⁷⁴

4.3. Enforcement in Banking (Central Bank of Ireland) (CBI)

The Central Bank of Ireland (CBI) is one of the most active regulators in investigating and issuing administrative financial sanctions in the EU. This stems from Ireland’s development in recent years as an ‘internationally focused financial centre’, with growth in ‘size, complexity, and interconnectedness’.⁷⁵ As a result, the entities and activities that fall within the remit of the CBI have also grown in scale and complexity.⁷⁶ The CBI has a long-established practice of issuing administrative financial sanctions.⁷⁷ In practice, most of these will result in ‘a settlement agreement’ as opposed to the CBI unilaterally imposing sanctions. In each case, both the Central Bank and the regulated entity are likely to have concluded that ‘the efficiency of entering a settlement agreement represented the best outcome’.⁷⁸ This in turn makes legal challenges to the courts less likely unless a regulated company or individual had a very robust complaint concerning a clear violation of any constitutional requirements as provided under Articles 34 and 37 of the Constitution.⁷⁹

⁷² Directive (EU) 2019/1. Ireland was one of 22 Member States that did not meet the transposition deadline in 2021: European Commission, Report on Transposition of Directive (EU) 2019/1, COM(2024) 558 final, 3.

⁷³ Competition Act 2002; Competition Act 2014.

⁷⁴ See Competition (Amendment) Act 2022.

⁷⁵ Bank of Ireland, *Fitness and Probity Review*, 11.07.2024. Otherwise known as the ‘Enria Report’, pp. 15-17 (Enria Report).

⁷⁶ *Ibid.*

⁷⁷ Law Commission Report 2018 (n 6) p. 112. Between 2004 and 2016, the CBI had issued financial sanctions in the region of 49.7 million EUR.

⁷⁸ *Ibid.*

⁷⁹ See discussion of *Zalewski* above.

In addition, the CBI has seen its supervisory and enforcement powers further enhanced through the Central Bank (Supervision and Enforcement) Act in 2013 and again, more recently, under the Central Bank (Individual Accountability Framework) Act 2023 (IAF Act). This included major national reforms to the legal and governance regime of the ‘Administrative Sanctions Procedure’ (ASP) applicable to individuals and companies when the CBI is investigating and sanctioning senior executives, and other employees, for violations of financial services rules. The new rules are set out in the IAF Act and associated guidelines (including the ‘Individual Accountability Framework’) (IAF).⁸⁰ The Act was signed into law in March 2023 and, following a public consultation, the IAF became fully applicable by July 2024.⁸¹ Two major cases influenced the recent reforms to the investigatory and enforcement powers underpinning the CBI’s updated Administrative Sanctions Procedure (ASP). The first was the 2021 landmark Irish Supreme Court employment law case in *Zalewski*, as noted above, and the second (with more significant specific implications for banking enforcement) was the *AB* case. This case concerned a 2024 decision by the Irish Financial Appeals Tribunal (IFSAT),⁸² which dealt with the CBI’s procedures for assessing fitness and probity applications of executives.⁸³ The CBI may refuse the appointment of a ‘pre-approval function’ role (PCF) applicant where the Bank is of the opinion that the person is not of such fitness and probity as is appropriate to perform the function for which he or she is proposed to be appointed.⁸⁴

Justice John MacMenamin, former judge of the Irish Supreme Court, delivered the significant and detailed IFSAT decision in *AB*. The case concerned a determination by IFSAT that the Central Bank of Ireland (CBI) had not applied ‘fair procedures’ in its assessment of whether the individual in question (*AB*) could be approved for two ‘pre-approval function’ (PCF) roles with an authorised investment fund. Questions regarding the constitutionality of the CBI procedures did not fall within the remit of the

⁸⁰ Central Bank (Individual Accountability Framework) Act 2023. The new legislation amends *inter alia* the Central Bank Act 1942, the Central Bank Reform Act 2010, and the Central Bank (Supervision and Enforcement) Act 2013.

⁸¹ Central Bank of Ireland, *Regulatory & Supervisory Outlook*, February 2025, p. 138.

⁸² IFSAT is a statutory body established under the Central Bank Act 1942, as amended by the Central Bank and Irish Financial Services Authority Act 2003 (CBIFSA Act). An individual, or regulated financial services provider, can appeal to IFSAT against any decision by the CBI identified as appealable in the legislation, including the imposition of administrative sanctions. IFSAT decisions can be appealed to the High Court.

⁸³ *AB v. The Central Bank of Ireland Decision*, IFSAT Appeal No. 029/2022, 15.03.2024. Note that MacMenamin J. also delivered the dissenting opinion in *Zalewski* (n 14).

⁸⁴ Applications for PCF positions are brought by financial service providers, generally investment funds.

IFSAT. However, consistent with *Zalewski*, the case also focused on ‘the question of fair procedures.’⁸⁵ The *AB* decision raised ‘issues regarding the Central Bank’s ‘handling of [the] application within the gate-keeping process, raising concerns about the effectiveness, fairness and transparency of the process.’⁸⁶ The *AB* has far-reaching implications for the regulation of financial service providers but also for the CBI as a regulator more widely. It promptly resulted in the CBI instigating an independent review of its ‘Fitness and Probity’ vetting framework undertaken and published shortly thereafter in 2024. The report was led by Andrea Enria, former chair of the European Central Bank, and made numerous recommendations concerning the investigatory and enforcement powers that underpin the CBI’s use of administrative sanctions.

Indeed, following the *AB* decision but prior to the Enria Report being published, the CBI had already introduced ‘interim enhancements’ to its F&P processes following the Supreme Court judgment in *Zaleswki*.⁸⁷ The legal regime underpinning the CBI Administrative Sanctions Procedure was amended to provide the following: 1) a person subject to investigation must be given an opportunity to make submissions on the CBI’s report on the outcome of a fitness and probity investigation; there must be limits to the category of people who can make significant decisions on fitness and probity; High Court confirmation is required *of any sanction* imposed following a CBI inquiry.⁸⁸ The *AB* decision poses important implications for a broader range of CBI decision-making across its investigatory and enforcement powers. As leading practitioners have observed, the decision highlighted the difficulty in reconciling the various functions that the Central Bank (CBI) carries out in line with the high standards set by the Supreme Court in *Zalewski* for non-judicial bodies exercising powers of administration of justice, such as administrative financial sanctions.⁸⁹ Consequently, the need for impartial, dispassionate and the independent exercise of key decision-making powers in accordance with fair procedures ‘extends to many of the appealable decisions’ identified in legislation concerning the powers of the Central Bank of Ireland.⁹⁰

⁸⁵ *AB* (n 83) p. 4.

⁸⁶ See Enria Report (n 75).

⁸⁷ *Ibid*, pp. 4-5.

⁸⁸ From 19 April 2023, all sanctions imposed by the CBI in relation to admissions-based settlements under the administrative sanctions procedure, set out in Part IIIC of the Central Bank Act 1942 (as amended), must be confirmed by the High Court in order for them to take effect.

⁸⁹ See, for instance, J. Grennan, ‘IFSAT – what’s that?!’, A&L Goodbody, 2024 online <https://www.algoodbody.com/insights-publications/ifsat-whats-that>.

⁹⁰ *Ibid*.

Overall, these measures are intended to ‘drive higher standards in governance, including accountability for decision-making and effective corporate culture in all firms.’⁹¹ The CBI can now, for instance, impose other sanctions, including lifetime work bans. On the other hand, legal practitioners ‘cautiously’ welcomed some of the main changes under the legal reforms to the ASP regime related to the due process rights of those under investigation by the CBI.⁹² These include ‘improving the rights of the defence at the investigation phase, more flexibility on its rules on confidentiality, permission to bring an independent legal representative at investigations, and better protection for legal privilege.’⁹³ The moves towards greater transparency and institutional governance may also prevent any potential risk of ‘investigation creep’ by the CBI from the original scope and principal purpose of its initial investigation.

4.4. Enforcement in VAT (Revenue Office)

Most of the statutory sanctions of the Revenue Office involve provision for payment of penalties on a specified basis depending on the nature (and scale) of the non-compliance or tax default. Authorised officers from the Revenue Office have numerous statutory powers allowing them to inspect any premises and access and procure any digital information (any ‘records’)⁹⁴ for the broad purposes of ‘any legal proceedings instituted by an officer of the Revenue Commissioners’.⁹⁵ Section 905(1) of the Taxes Consolidation Act 1997 (Act of 1997) broadly defines records as: ‘any document or any other written or printed material in any form, including *any information stored, maintained or preserved by means of any mechanical or electronic device*, whether or not stored, maintained or preserved in a legible form, which a person is obliged by any provision relating to tax to keep, retain, issue or produce for inspection or which may be inspected under any provision relating to tax’.⁹⁶ The information gathering powers of the Revenue Office became operational in 1999. They are notably broadly framed in scope and were adopted with the primary aim of tackling tax evasion.⁹⁷

The far-reaching scope of these information powers clearly provide for requesting data from third parties, such as OSPs, for the purposes of VAT

⁹¹ Central Bank of Ireland, *Regulatory & Supervisory Outlook*, February 2025, p. 126.

⁹² Law Society of Ireland, *Update on Changes to the CBI’s Administrative Sanctions Procedure Business Law Committee*, February 2024.

⁹³ *Ibid.*

⁹⁴ See generally Part 38, Chapter 4 of the Taxes Consolidation Act 1997.

⁹⁵ See, for instance, Taxes Consolidation Act 1997, section 904.

⁹⁶ Emphasis added.

⁹⁷ Revenue Office, *Guidance on Revenue Information Powers* (last updated August 2024) [online revenue.ie/en/tax-professionals/tdm/powers/38-04-04.pdf](https://online.revenue.ie/en/tax-professionals/tdm/powers/38-04-04.pdf).

enforcement. The Act of 1997 states that an officer of the Revenue Office may in the exercise or performance of his or her powers or duties ‘require any person having charge of, or otherwise concerned with the operation of, the data equipment or any *associated apparatus or material*, to afford him or her *all reasonable assistance* in relation to the exercise or performance of those powers or duties.’⁹⁸ Regarding VAT enforcement, sections 902, 902A and 907A of the Act of 1997 TCA confer powers on an authorised officer to require a third party, other than a financial institution, to deliver books, records and other documents and to provide information in relation to a taxpayer in certain circumstances. The power to give notice directly to a third party under section 902 requires the consent of a Principal Officer/Branch Manager. Section 902(3) provides that the authorised officer must have ‘reasonable grounds’ to believe that the third party (who may or may not be connected to the tax payer) is likely to have information relevant to the establishment of a liability in relation to the ‘taxpayer’, before serving a notice under this section.

Section 902(10) requires a person who, in compliance with a notice under this section makes books, records, or other documents, available for inspection by an authorised officer to afford the officer reasonable assistance. This includes information ‘in relation to the use of all electronic or other automatic means’ by which the books, etc, in non-legible form are capable of being reproduced in legible form. A penalty of 4,000 EUR is provided in section 902(11) for the refusal or failure by a person to comply with a notice under this section, or for failure to give the assistance provided for in this section.⁹⁹

5. TRANSFER OF DATA BETWEEN PROCEEDINGS

5.1. Transfers of data between national proceedings and authorities

There are no binding legal requirements which make the transfer of data between national proceedings and authorities mandatory. However, there are broadly framed provisions within the relevant statutory regimes of the numerous competent authorities which provide that different competent authorities ‘may’ cooperate with each other and exchange information generally for various purposes. For instance, the Competition Amendment

⁹⁸ See section 912(3) of the Taxes Consolidation Act 1997, as amended. Section 912(1) defines data equipment as ‘any electronic, photographic, magnetic, optical or other equipment for processing data’ (emphasis added).

⁹⁹ See Section 902 Taxes Consolidation Act 1997, Request of an authorised officer: information to be furnished by a third party, Tax and Duty Manual, Revenue Commissioners Office (last updated November 2024) online <https://www.revenue.ie/en/tax-professionals/tdm/powers/38-04-04f.pdf>.

Act 2022 provides that the CCPC and ComReg ‘may’ cooperate, ‘including by sharing information and evidence between them’, with respect to putting together programmes that OSPs may refer to in order to seek ‘leniency’ from administrative sanctions resulting from serious competition law infringements (cartel involvement).¹⁰⁰ In practice, this means that there is no culture of data transfers between national authorities as the authorities in question will instead go directly to an OSP for any necessary digital information due to what has now become a deeply entrenched voluntary cooperation regime.¹⁰¹

5.2. Transfers of data between foreign and national proceedings

There is no binding legal basis in Irish law (other than a Mutual Legal Assistance Treaty)¹⁰² which specifically makes the transfer of data between national proceedings and foreign authorities mandatory.¹⁰³ However, the broad information powers of the Revenue Commissioners to request data from OSPs, as noted above, may also be used for ‘assisting the prevention and detection of tax evasion, by means of the exchanges of information between the Revenue Commissioners and the tax authorities of certain other territories’.¹⁰⁴ In addition, there are broadly framed provisions within legally non-binding Memoranda of Understanding (MoU) between numerous Irish competent authorities (in Europe and beyond) which provide that different competent authorities ‘may’ cooperate with each other and exchange information generally for various purposes. The US Federal Trade

¹⁰⁰ See section 15AI (9), Competition (Amendment) Act 2022.

¹⁰¹ See generally McIntyre (n 4).

¹⁰² The only mechanism would be through the existence of an MLAT (Mutual Legal Assistance Treaty) *via* the Gardai (Irish police) Where there is the case, such as the EU-US MLAT, the EDPB states that ‘EU companies should generally refuse direct requests and refer the requesting third country authority’ to the MLAT process. See EDPB and EDPS, “Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection”, “Annex, Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence”, 10 July 2019 online edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en. See J.D. Michels, C. Millard, I. Walden, et al., ‘Cloud Sovereignty and the GDPR, Part One: US Government Access to European Data’, p. 28, *SSRN Journal*, 2024, online https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4911552.

¹⁰³ McIntyre (n 4) makes the argument that a possible legal basis could be a disclosure to protect the ‘vital interests’ of a natural person under Article 6(1)(d) GDPR.

¹⁰⁴ Finance Act 2013, section 99 (amending section 912 of the Act of 1997).

Commission (FTC) and the DPC have such an arrangement in a MoU adopted in 2013.¹⁰⁵

5.3. Admissibility of data collected from OSPs as third parties as evidence

Admissibility of data collected from OSPs as third parties to an investigation involving the imposition of administrative financial sanctions by regulators in Ireland is a complex area as there is no codified law on the provision of digital evidence and such information is (in most cases) provided on a voluntary basis. The admissibility of evidence obtained through mandatory cooperation using a warrant in criminal proceedings has been successfully challenged in the Irish Courts.¹⁰⁶ A defendant could also challenge the admissibility of evidence gathered this way in subsequent criminal proceedings and the Irish exclusionary rule will mean that such evidence may be excluded if it was obtained illegally or unconstitutionally.¹⁰⁷ The Competition (Amendment) Act 2022 states, whether in criminal or civil proceedings, that ‘electronic messages’ or related information (in the broadest of scope) are admissible evidence.¹⁰⁸ This provision only recently entered into force in 2023 and has not yet been tested in terms of its potential future scope and application to the admissibility and gathering of digital evidence from OSPs as third parties to an investigation.

6. CONCLUSION

Administrative financial sanctions are an established element in the regulatory toolkit of regulators of most legal systems in the EU with Ireland being a relatively late arrival to this practice. This shift has been primarily instigated by a growing wave of EU legislation which provide for the imposition of these sanctions by competent authorities in the exercise of their

¹⁰⁵ FTC Press Release, 27 June 2013, online [ftc.gov/news-events/news/press-releases/2013/06/ftc-signs-memorandum-understanding-irish-privacy-enforcement-agency](https://www.ftc.gov/news-events/news/press-releases/2013/06/ftc-signs-memorandum-understanding-irish-privacy-enforcement-agency).

¹⁰⁶ As held by the Irish Supreme Court in *CRH Plc, Irish Cement Ltd v Competition and Consumer Protection Commission* [2017] IESC 34.

¹⁰⁷ See Y.M. Daly, 'Overruling the Protectionist Exclusionary Rule: DPP v JC', *International Journal of Evidence & Proof*, 2015, vol. 19, p. 270, DOI:10.1177/1365712715601764; McIntyre and Murphy (n 9). In terms of other constitutional protections, the Irish courts have established that body corporates have a right to fair trial: *Criminal Assets Bureau v Mac Aviation Ltd* [2010] IEHC 121.

¹⁰⁸ Section 15AW, Competition (Amendment) Act 2022 states: ‘The types of proof that are admissible as evidence in proceedings under this Act (whether criminal or civil, including proceedings under Part 2 and Parts 2C to 2F before a court or an adjudication officer) shall include relevant documents, oral statements, electronic messages, recordings and all other objects containing information, irrespective of the form it takes and the medium on which information is stored, provided that the proof would be admissible before a court.’

investigatory and enforcement powers. Major legislative reforms in this area include the significant administrative financial sanction powers that may now be imposed in the areas of data protection enforcement and more recently competition law enforcement. The longer-established, and frequently used, significant administrative financial sanction powers of the Central Bank of Ireland (CBI) have also been enhanced in recent legislation. These have also been introduced in tandem with a shift towards greater transparency and due process safeguards in the exercise of the CBI's investigatory and decision-making powers and its institutional operation. This shift applies across all enforcement powers of the CBI, including administrative financial sanctions. These reforms, and related reforms in other sectors, such as the Competition (Amendment) Act 2022, follow two major legal cases. The landmark judgment of the Irish Supreme Court in 2021 (*Zalewski*) and the influential IFSAT decision in 2024 (*AB*) both concerned administrative bodies and the high standards they must meet with respect to the fair procedures to be applied in the exercise of their investigatory and enforcement powers. It remains to be seen how these developments will be addressed by the courts in future with respect to any cases concerning administrative financial sanctions. Three key factors at play here for individuals/entities considering such proceedings comprise: the significant cost of such proceedings; the risk of reputational damage for any individuals or companies involved; and, following *Zalewski*, how the courts will approach the discretion afforded to administrative bodies in determining the relevant constitutional safeguards to be applied when exercising their powers in the administration of justice.

9. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN ITALY

G. LASAGNI

1. COMPETENT AUTHORITIES IN SELECTED AREAS OF PUNITIVE ADMINISTRATIVE ENFORCEMENT¹

There is no general framework regarding punitive administrative proceedings in Italian law. Although the *Engel* doctrine² finds application at the domestic level, either to apply specific decisions issued by the European Court of Human Rights (ECtHR), or at the own initiative of national courts, this occurs only on a case-by-case basis. Thus, the concrete identification of both i) the precise scope of the punitive matter and ii) the identification and scope of the rights of the accused in such proceedings is not clearly foreseeable *ex ante*.

As illustrated below, sectoral legislation generally does not explicitly recognise the punitive nature of specific sanctions either. Thus, none of the enforcement areas studied in this research is officially classified as punitive under Italian law. Nonetheless, in several instance specific procedural safeguards have been introduced or strengthened precisely to address the concerns arising from the application of the *Engel* doctrine. The latter, however, is not a trend that concerns equally all the domains considered here. For instance, a key aspect, such as the privilege against self-incrimination in punitive proceedings, is only seldom considered in the areas examined below, and to a diverging extent.

However, a common trait that characterises the selected Italian enforcement areas is the presence of a ‘double track’ system. Indeed, most breaches tend to be sanctioned both by criminal and administrative law. The distinction between the two is often represented by the gravity of the conduct (more severe: criminal punishment, less severe: administrative punishment); however, no systematic or common approach that clearly defines the sanctioning policy concerning the punitive matter may be found.

¹ The present chapter was last updated in January 2025.

² ECtHR, *Engel and others v. The Netherlands*, 08.06.1976, no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72, § 80 and followings.

Against this fragmented background, enforcement authorities' powers vary greatly from one to another. In most cases, such authorities enjoy mixed enforcement powers, though even the way in which such mixing is appreciable also varies from sector to sector.

In customs, enforcement powers are being exercised by the Customs and Monopolies Agency (*Agenzia delle Dogane e dei Monopoli* - ADM). This body was established in 2012, after the unification of the Customs Agency and the Autonomous Administration of State Monopolies,³ and its enforcement powers are regulated by a variety of legislative acts.⁴ ADM is an administrative authority that extends its competence over several areas, namely customs, movement of goods, excise duties, monopolies, and gambling. In performing their duties, ADM officials may also assume the role of judicial police officers. This status enables customs officials to conduct criminal investigations related to breaches of customs excises, duties, and monopolies law, including seizures and the collection of documents and information, or performing arrests.⁵ In this regard, ADM may be considered an entity with mixed (criminal and administrative) nature concerning investigations. Yet, ADM may only impose administrative penalties, while criminal sanctions are applied only by judicial authorities. Thus, for what

³ See Article 23-*quater*, Law Decree no. 95 of 06.07.2012 *Disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini (nonché misure di rafforzamento patrimoniale delle imprese del settore bancario)*.

⁴ Among which, the most relevant for the present research are: Presidential Decree no. 43 of 23.01.1973 *Testo unico delle disposizioni legislative in materia doganale*; Legislative Decree no 374 of 08.11.1990 (*Riordinamento degli istituti doganali e revisione delle procedure di accertamento e controllo in attuazione delle direttive n. 79/695/CEE del 24 luglio 1979 e n. 82/57/CEE del 17 dicembre 1981, in tema di procedure di immissione in libera pratica delle merci, e delle direttive n. 81/177/CEE del 24 febbraio 1981 e n. 82/347/CEE del 23 aprile 1982, in tema di procedure di esportazione delle merci comunitarie*); Legislative Decree no 471 of 18.12.1997 (*Riforma delle sanzioni tributarie non penali in materia di imposte dirette, di imposta sul valore aggiunto e di riscossione dei tributi, a norma dell'articolo 3, comma 133, lettera q), della legge 23 dicembre 1996, n. 662*); Law Decree no 223 of 04.07.2006 *Disposizioni urgenti per il rilancio economico e sociale, per il contenimento e la razionalizzazione della spesa pubblica*; and Legislative Decree no. 141 of 26.09.2024 *Disposizioni nazionali complementari al codice doganale dell'Unione e revisione del sistema sanzionatorio in materia di accise e altre imposte indirette sulla produzione e sui consumi. (24G00156)*.

⁵ Pursuant to Articles 57, § 3 CCP; Articles 324 and 325, Presidential Decree 43/1973; Articles 30 and 31 of Law 4/1929, Article 32 of Legislative Decree 331/1993 conv. into Law 427/1993 and Articles 18, 19 and 58 of Legislative Decree 504/1995 ('Consolidated Law on Excise Duties'). By the Decree Law no. 23 of 08.04.2020, the functions of the judicial police were extended to personnel attached to the Monopolies. On the matter, see F. Tarini, 'Aspects of Customs Controls Performed by the Italian Customs Authority' in: G. D'Angelo (ed.), *Aspects of Customs Control in Selected EU Member States*, Bologna University Press, 2023, p. 24 and followings.

concerns the sanctioning powers, ADM may be considered an administrative body.

The area of VAT tax enforcement is characterised by a significant degree of complexity under Italian law, given by the interaction of several pieces of statutory law,⁶ as well as the concurring competence of diverse administrative authorities. More specifically, the investigation of administrative violations of tax laws, including VAT, is the responsibility of 'tax police' (*polizia tributaria*), as well as other bodies specified in individual laws, having been vested with the cognisance of tax, criminal and administrative violations.⁷ With regard to administrative investigations on VAT,⁸ the competent enforcement authorities range from bodies with (also) clear criminal law enforcement powers, such as the Italian military economic police *Guardia di Finanza* (GDF),⁹ to administrative bodies with mixed powers, such as the Revenue Agency (*Agenzia delle Entrate*).

On the one hand, GDF is a military body of financial law enforcement, that has a hybrid nature: it may operate as an administrative body and carry out administrative investigations in case of VAT administrative breaches. Still, it may also operate as a body of judicial police, thus investigating criminal tax offences in accordance with the criminal procedure rules. On the other hand, the Revenue Agency is an administrative authority, operational since 1st January 2001, and created as a result of the reorganisation of the financial administration.¹⁰ Its officers are empowered to conduct access, inspections, audits and searches to assess tax and suppress evasion and other violations. Officers of the financial agencies, including the Revenue Agency, and ADM, may be entrusted with the enforcement of VAT sanctions. Such officers may also have a hybrid status: while they investigate administrative

⁶ The regulatory source of the enforcement powers of these authorities is not contained in an organic text, having to refer instead to individual tax laws. For the purposes of this study, the main legal bases are represented by Presidential Decree no. 633 of 26.10.1972 *Istituzione e disciplina dell'imposta sul valore aggiunto*, and by Law no. 4 of 07.01.1929, as well as - for what concerns sanctions - by Legislative Decree no 471 of 18.12.1997 *Riforma delle sanzioni tributarie non penali in materia di imposte dirette, di imposta sul valore aggiunto e di riscossione dei tributi, a norma dell'articolo 3, comma 133, lettera q), della legge 23 dicembre 1996, n. 662*. G. U. 8 gennaio 1998, n. 5, - S.O. 4 (administrative sanctions) and by Legislative Decree no. 74 of 10.03.2000 *Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della legge 25 giugno 1999, n. 205* (criminal sanctions).

⁷ As stipulated by Article 34 of Law 4/1929.

⁸ For tax criminal offences, also ordinary law enforcement agencies may be involved, see Article 32 ff, Law 4/1929.

⁹ See Article 31, Law 4/1929.

¹⁰ Following Legislative Decree no. 300/1999.

(also) VAT breaches,¹¹ they can receive the status of judicial police officers in relation to certain criminal investigations.¹²

In the area of banking and financial markets, as well as in competition law and GDPR enforcement, the competence is entrusted to independent administrative authorities, namely the Italian Banking Supervisory Authority (*Banca d'Italia*), the Italian Financial Market Supervisory Authority (*Commissione Nazionale per le Società e la Borsa* - Consob), the Italian Competition Authority (*Autorità Garante della Concorrenza e del Mercato* - AGCM), and the Italian Data Protection Authority (*Garante per la protezione dei dati personali* - GPD). respectively. Such authorities can impose only administrative sanctions, although some can be considered substantially criminal in light of the *Engel* doctrine, or at least punitive.

More specifically, Banca d'Italia is the independent administrative body competent to investigate and issue punitive sanctions in the area of banking supervision. In addition to the relevant EU legislation, at the domestic level, the sanctioning powers of Banca d'Italia are regulated by the Consolidated Banking Law (TUB)¹³ and by the Consolidated Financial Law (TUF),¹⁴ as well as by several internal regulations.¹⁵ Banca d'Italia has an administrative nature. Consequently, it formally can impose administrative sanctions only. Nonetheless, the nature of the latter has often been questioned both by the case law and by legal scholars, and this debate has led to the recognition of the punitive nature of some sanctions imposed by Banca d'Italia.¹⁶ Sanctions that are officially classified as criminal by the law, on the other side, are left to the competence of the judicial authorities exclusively.

Consob is the administrative authority competent to investigate and issue sanctions in financial market law. In addition to relevant EU legislation,

¹¹ See Article 52, Presidential Decree 633/1972.

¹² Pursuant to Article 57 CCP, according to which all persons in charge of investigating and ascertaining certain kinds of crimes are to be considered officers or agents of the judicial police, within the limits of the service to which they are assigned and according to the powers conferred on them by laws or regulations. See also Article 75, Presidential Decree 633/1972.

¹³ Articles 50 and followings, *Testo Unico Bancario* (TUB) Legislative Decree no. 385 of 01.09.1993 (lastly amended by Law Decree no. 69, 13.06.2023).

¹⁴ Articles 130 and followings, *Testo Unico delle disposizioni in materia di intermediazione finanziaria* (TUF), Legislative Decree no. 58 of 24.02.1998 (lastly amended by Law no. 21 of 05.03.2024, in force since 27.03.2024).

¹⁵ Specifically, Act of 18.12.2012, *Disposizioni di vigilanza in materia di sanzioni e procedura sanzionatoria amministrativa*, as subsequently amended (lastly on 27.07.2022). All regulations and acts are published on the Banca d'Italia website (<https://www.bancaditalia.it/compiti/vigilanza/normativa/index.html?dotcache=refresh#3>); for the sanctioning regulations and acts, see specifically: <https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/pro-sanz/index.html>.

¹⁶ For more details see below, Section 2.2.3.

at the domestic level, the sanctioning powers of Consob are also regulated by TUB¹⁷ and TUF,¹⁸ as well as by several internal regulations.¹⁹ Consob has an independent and administrative nature, and consequently can impose only administrative sanctions. Regardless, the same debate about the substantial nature of Banca d'Italia's sanctioning powers extended to Consob's, with rather similar results.²⁰ Formally, criminal sanctions, also in this domain, are left to the application of the judicial authorities exclusively.

AGCM is the independent administrative authority competent to investigate and issue sanctions in the area of competition law enforcement.²¹ Although all sanctions that AGCM may impose have a formal administrative nature, some of them have been recognised as having a substantial criminal nature by the case-law, in light of the *Engel* criteria.²² Interestingly, with regard to natural persons, the Italian legal framework on competition law explicitly mentions the category of 'punitive sanctions', though without defining exactly what the expression refers to.²³

Last, GPDG is the body entrusted with investigating and punishing GDPR violations. GPDG is an independent administrative authority, established in 1996²⁴ and then comprehensively regulated by the so-called Italian "Privacy Code" since 2003.²⁵ The GPDG's enforcement powers are of

¹⁷ Article 130 and followings TUB.

¹⁸ Article 166 and followings TUF.

¹⁹ Namely, Consob Regulation no. 11971 of 14.05.1999 *di attuazione del decreto legislativo 24 febbraio 1998, n. 58 concernente la disciplina degli emittenti (aggiornato con le modifiche apportate con delibera n. 23016 del 20 febbraio 2024, in vigore dal 29 febbraio 2024)*; Consob Regulation no. 20249 of 28.12.2017 *recante norme di attuazione del decreto legislativo 24 febbraio 1998, n. 58 in materia di mercati (aggiornato con le modifiche apportate con delibera n. 22804 del 6 settembre 2023, in vigore dal 19 settembre 2023)*; and Consob Regulation no. 20307 of 15.02.2018 *recante norme di attuazione del decreto legislativo 24 febbraio 1998, n. 58 in materia di intermediari (modificato con delibera n. 22430 del 28 luglio 2022, in vigore dal 16 agosto 2022)*.

²⁰ For more details see below, Section 2.2.3.

²¹ Established by Law no. 287 of 10.10.1990 *Norme per la tutela della concorrenza e del mercato*.

²² Also at the European level, see famously, ECtHR, *A. Menarini Diagnostics S.r.l. v. Italy*, 27.09.2011, no. 43509/08.

²³ Article 14, § 2, Law 287/1990.

²⁴ Law no. 675 of 31.12.1996.

²⁵ I.e. Legislative Decree no. 196 of 30.06.2003 *Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*. The Privacy Code was recently amended by Legislative Decree no. 101 of 10.08.2018 to ensure coordination with the General Data Protection Regulation (EU) 2016/679. Such Decree confirmed that the GPDG is the designated supervisory authority also for the purpose of implementing GDPR (Article 51).

administrative nature, although some of the sanctions under privacy law (especially after the entrance into force of the GDPR) may be considered rather criminal in substance. After the entry into force of the GDPR, the GPDp's investigative powers are largely regulated directly by EU law.

2. PUNITIVE ADMINISTRATIVE PROCEEDINGS: SECTORAL FRAMEWORK

In most selected areas of law, the Italian legal framework does not provide for specific powers of competent authorities to request data that is available to online service providers (OSPs), except for the areas of financial market law and competition law.

2.1. Requests for data to OSPs

2.1.1. Financial market law

In the scope of market abuse, the legislation grants Consob the power to request specific types of electronic evidence from a vast array of subjects. Namely, Consob may:²⁶ 1) request to anyone that might be informed about the facts to be ascertained, the production of existing recordings of telephone conversations, electronic communications, and data exchange; 2) directly access, by means of an appropriate telematic connection, the data contained in the lists referring to the facilities of the owner of electronic communication infrastructures;²⁷ 3) request the acquisition from the provider of the traffic data referred to in the Privacy code,²⁸ or directly acquire such data through a telematic connection; and 4) request the disclosure of personal data (which arguably may take an electronic form as well), also in derogation of the prohibitions laid down in the Privacy code.²⁹

²⁶ In accordance with Article 187-*octies* TUF (see § 3, let b) for no. 1; and § 4 for no. 2 ff).

²⁷ Article 55(7) of Legislative Decree no. 259 of 01.08.2003 (*Codice delle comunicazioni elettroniche*). The notion of “owner of electronic communication infrastructure” is not fully defined by the legislation, in as much as Article 2, let. t-*ter*), Legislative Decree 259/2003 defines the notion of “electronic communications equipment” as a set of network devices comprising the equipment and infrastructure necessary for the transmission, reception and processing of electronic signals, but it does not explicitly circumscribe the notion of ownership in this regard. Still, also due to the broadness of the definition, OSPs seems easily included in the notion.

²⁸ Defined by Article 121(1-*bis*), let h) Legislative Decree 196/2003 as any data processed for the purpose of the transmission of a communication over an electronic communications network or the billing thereof.

²⁹ Article 25(1) of Legislative Decree 196/2003. Consob may also: 6) make use, where necessary, of the data contained in the register of accounts and deposits (referred to in Article 20(4) of Law no. 413 of 30.12.1991, in accordance with the modalities set out in Article 3(4)(b) of Decree-Law no. 143 of 03.05.1991, converted, with amendments, into Law no.

The scope of Consob's powers listed is limited to investigations related to market abuse (in light of Regulation (EU) No 596/2014³⁰ and the TUF). In this area, the conditions under which data may be requested are provided in very broad terms by the TUF, as it allows Consob to perform all acts necessary to investigate potential administrative breaches.³¹

To acquire traffic data from the provider, the law requires Consob to obtain an authorisation from a prosecutor.³² Where the request is addressed to subjects not under Consob's supervision (considering Regulation (EU) no. 596/2014), such authorisation is also necessary to obtain existing recordings of telephone conversations, electronic communications, and data exchange. In a broader perspective, the need to receive such an authorisation may appear problematic. Indeed, since 2021, the regulation concerning access to communications metadata for criminal investigation purposes has been amended, and it currently requires obtaining an authorisation from a judge, rather than a prosecutor.³³ The same amendment, however, has not been introduced to the TUF.

413 of 30.12.1991, in accordance with Article 3(4)(b) of Decree-Law no. 413 of 30.12.1991), as well as acquire, also through direct access, the data contained in the archive containing the information about persons carrying out transactions involving the transmission or handling of means of payment of any kind whatsoever that are in excess of twenty million liras [sic: amount not expressed in EUR in the legislation] in a series of determined contexts (specifically: (a) public administration offices, including post offices; (b) credit institutions; (c) stockbroking companies; (d) commission agents admitted to the anti-collection lists of stock exchanges; (e) stockbrokers; (f) companies authorised to carry out door-to-door sales of securities; (g) management companies of investment funds; (h) trust companies; (i) insurance companies and entities; l) *Monte Titoli S.p.a.* companies; (m) intermediaries having as their main purpose, or performing one or more of the following activities: granting of financing in any form, including leasing; acquisition of equity interests; foreign exchange intermediation; collection, payment and funds transfer services also by means of issuance and management of credit cards; (m-bis) electronic money institutions), or the persons on whose behalf they may be carrying out the transaction (Article 13 of Law Decree no. 625 of 15.12.1979, converted, with amendments, by Law no. 15 of 06.02.1980); 7) directly access, by means of an appropriate telematic connection, the data contained in the Centrale dei Rischi of the Banca d'Italia (referred to in the resolution of the Interministerial Committee for Credit and Savings of 29.03.1994, published in the Official Gazette no. 91 of 20.04.1994); and 8) make use, where necessary, also by telematic connection, of the data contained in the special section of the tax registry (referred to in Article 7, § 6, of Presidential Decree no. 605 of 29.09.1973).

³⁰ Regulation (EU) no 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.

³¹ See Article 187-octies, § 2, TUF.

³² See Article 187-octies, § 6, TUF.

³³ See Article 132 of Legislative Decree no. 196/2003, as amended by Law Decree no. 132 of 30.09.2021.

As far as the rules of data transfer are concerned, national legislation states that, for existing recordings of telephone conversations, electronic communications, and data exchange, Consob shall establish at its discretion the deadlines for the transmission of the data.³⁴

For the supervisory tasks that exceed market abuse (from crowdfunding to intermediaries³⁵), the TUF confers a series of investigative powers to Consob, among which are included some of those already mentioned above (namely, to access directly, by means of an appropriate telematic connection, the data contained in the lists referring to the facilities of the owner of electronic communication infrastructures; to request the acquisition from the provider of the traffic data referred to in the Privacy code, or directly acquire such data employing telematic connection; and to request the disclosure of personal data (which arguably may take an electronic form as well), also in derogation of the prohibitions laid down in the Privacy code).³⁶ Contrary to the case of market abuse, all these powers may be used only against supervised entities. Yet, the request for communications data is drafted differently.

Consob here may only request existing records relating to telephone conversations, electronic communications or data exchanges held by a supervised subject; and records held by a telecommunications operator concerning telephone conversations and data exchanges of a supervised subject.³⁷ Contrary to the area of market abuse, in this context, a prosecutorial authorisation is necessary only for records held by a telecommunications operator; thus, not for existing records relating to telephone conversations, electronic communications or data exchanges held by a supervised subject.³⁸ Terms and deadlines are determined by Consob in these cases.³⁹ In the exercise of all the requesting powers discussed, Consob may avail itself of the support of Guardia di Finanza, which carries out the requested investigations acting with the powers of inquiry attributed to it for the purposes of assessing value added tax (VAT).⁴⁰

No specific rules concerning sanctions and enforcement mechanisms referring to electronic evidence are provided for in Consob's investigations; however, some general norms, common to the banking law sector, are

³⁴ Article 187-*octies*, § 3, let b) TUF.

³⁵ For a complete list, see https://www.consob.it/c/portal/layout?p_l_id=12011&p_v_l_s_g_id=0.

³⁶ Article 6-*bis*, § 5 TUF, referring to the powers listed in Article 187-*octies* under nos. 2, 3, 4, 5, 6, and 7.

³⁷ According to Article 6-*bis*, § 5, let b) and c) TUF.

³⁸ See Article 6-*bis*, § 7.

³⁹ See Article 6-*bis*, § 4.

⁴⁰ See Article 187-*octies*, § 12 and Article 6-*bis*, § 9.

explained in detail below, specifically referencing to the right against self-incrimination (Section 2.2.3).

Also, no specific rules or remedies are provided with exclusive regard for electronic evidence, or OSPs. Nonetheless, when Consob carries out its investigation in the domain of market abuse (thus, also exercising the power to request communications data), the provisions of Articles 199, 200, 201, 202 and 203 of the Code of Criminal Procedure (CCP) shall apply, to the extent possible, *mutatis mutandis*.⁴¹ Such provisions refer to the possibility or the duty to invoke secrecy when requested by the authority to provide information; however, the extent to which the latter apply to OSPs seems relatively limited. In particular, they might become relevant should the OSP doubt that the information requested by the authority is covered by State secrecy (for instance, in case a communication involves persons holding public offices that might fall under such protection).⁴²

2.1.2. Competition law

The other area of law where specific powers to request data available to OSPs are established is competition law, and more specifically in investigation concerning abuse of dominant position and cartels.⁴³

In this domain, the AGCM shall take its decisions by assessing the elements in its possession and those brought to its attention by public administrations or any person with an interest therein. The law explicitly mentions documents, oral statements, electronic messages, recordings and all other documents containing information, regardless of their form and the medium on which the information is stored.⁴⁴ The obligation to provide all necessary information includes information accessible to the addressees of the request, which, especially in light of the nature of the information at stake, can also encompass OSPs.⁴⁵

Such requests to produce information and documents can be issued by the AGCM at any time during the investigation. Undertakings, associations

⁴¹ In accordance with Article 187-*octies*, § 7 TUF. More specifically, for what concerns private individuals: Article 199 confers a faculty to abstain from providing information (*facoltà di astensione*) to the family members of the accused; Article 200 refers to the possibility of invoking professional secrecy by private individuals; Article 202 refers to the obligation not to provide information covered by State secrecy, and Article 203 to the faculty of law enforcement and secret service members not to reveal the name of their informants (given that in such case, the information obtained by such individuals cannot be used as evidence at trial).

⁴² Such as the Members of Parliament, or President of the Republic (some

⁴³ Article 12, §§ 1 and 1-*bis*, Law 287/1990; see also Articles 2 and 3, Law 287/1990, and Articles 101 and 102 TFEU.

⁴⁴ See Article 12, § 1*bis*, Law 287/1990.

⁴⁵ See Article 14, § 2, Law 287/1990.

of undertakings or natural and legal persons possessing such information should be given a reasonable time limit to comply. The time limit shall be indicated in the request and is not set by law.⁴⁶ The requests for information are issued at AGCM's discretion and are not subject to any authorisation. According to some legal scholars, non-cooperation with the AGCM could also be sanctioned by criminal law.⁴⁷ Still, such requests shall be proportionate and not oblige the addressees to admit an infringement of competition law rules.⁴⁸

In addition to this specific power, the AGCM may also request information to a larger extent, both in the matter of abuses of dominant position and cartels,⁴⁹ as well as in investigations concerning concerted practices.⁵⁰

In these cases, the authority may request information and order the production of relevant documents from undertakings and entities with access to such information.⁵¹ Although the term 'entities' (*enti*) does not explicitly refer to OSPs, in principle it could also encompass such private actors.

Also, such requests to produce information and documents are issued by the AGCM at any time during the investigation, without any specific condition or authorisation. The AGCM shall grant the requested persons an adequate period to comply with it, considering of the complexity of the information in question. The time limit shall not exceed 60 days, but it is renewable by a reasoned request if that is necessary to reply to the demands issued by the authority.⁵²

The requests for information shall state the legal grounds on which they are based, shall be proportionate, and, according to the law, shall not oblige

⁴⁶ See Articles 14, § 2, Law 287/1990.

⁴⁷ In light of Article 2638 c.c. (as in relation to Banca d'Italia and Consob, see below, Section 2.2.3), given the broad reference to 'supervisory functions' in the text of such provision, see P. Severino, 'Le sanzioni antitrust tra diritto amministrativo e diritto penale: la visione del penalista' *Aperta Contrada*, 2014.

⁴⁸ Conversely, in accordance with Article 14, § 5, let. d) Law 287/1990, the AGCM may sanction (with a fine of up to 1% of the total worldwide turnover achieved during the preceding financial year) the undertakings or associations of undertakings that, intentionally or negligently, provide incorrect, incomplete or misleading information or do not provide the information within the prescribed time limit. The AGCM may also impose periodic pecuniary penalties (of up to 5 per cent of the average daily worldwide turnover in the preceding business year for each day of delay from the date fixed in the request or order), to compel the same subjects to provide complete and accurate information in response to a request for information (see Article 14, § 6, Law 287/1990).

⁴⁹ See Articles 2 and 3, Law 287/1990, and Articles 101 and 102 TFEU.

⁵⁰ See Article 16-bis, § 1, Law 287/1990.

⁵¹ See Article 12, § 2-bis, Law 287/1990.

⁵² In accordance with Article 12, § 2-ter, and Article 16-bis, § 2, Law 287/1990.

the addressees to admit an infringement of competition law.⁵³ No specific remedies are however foreseen to protect the interests of such persons. Moreover, the persons who are requested to provide or exhibit the elements referred to above shall be subject to pecuniary administrative sanctions if they refuse or omit to provide the information or to exhibit the requested documents, or if they provide untruthful information or display untruthful documents without a justified reason.⁵⁴ Such administrative fines amount to 1 % of the total worldwide turnover achieved during the preceding financial year.⁵⁵

The Italian legislation does not provide specific rules concerning requests for information from foreign addressees in this context. In general, in relation to investigations on abuse of dominant position and cartels, the AGCM may exercise its investigatory powers on behalf and for the account of other antitrust authorities of EU Member States. These may request the AGCM to investigate any failure by undertakings or associations of undertakings to comply with their requests for information, inspections, summonses to a hearing, warnings, interim measures, and decisions with commitments adopted by the requesting authority about the application of Articles 101 and 102 TFEU.

In turn, the AGCM may request the national competition authorities of EU Member States to exercise their powers of investigation to collect information referring to Italian proceedings.⁵⁶ Within such a cooperation system, though in the absence of specific provisions, it is plausible to conclude that requests for information regarding foreign OSPs will be enforced in application of the local domestic law. Thus, in principle, the risk of conflicting legal obligations stemming from differences among legal systems should be avoided. When information is collected abroad, the national legislation explicitly states that the latter shall be admitted as

⁵³ See Articles 12, § 2-*bis* and 16-*bis*, Law 287/1990.

⁵⁴ *Idem*.

⁵⁵ As established by Article 14, § 5, Law 287/1990. They refer to the following intentional or negligent obstructive conducts: a) undertakings or associations of undertakings obstruct the inspection (Article 14, § 2-*quarter*); b) seals affixed are broken, without prejudice to further criminal sanctions for the offender (Article 14, § 2-*quater* (d)); c) in response to a request made in the course of an inspection, undertakings and associations of undertakings fail to provide a complete answer or provide incorrect or misleading information (Article 14, § 2-*quater* (e), Law 287/1990); d) in response to a request for information, undertakings and associations of undertakings provide incorrect, incomplete or misleading information or do not provide the information within the prescribed time limit (Article 14, § 2); e) the undertakings or associations of undertakings fail to appear at the hearing convened (Article 14, § 2-*bis*).

⁵⁶ Article 15-*octies*, Law 287/1990.

evidence in domestic proceedings, subject to the safeguards laid down in Article 12 of Regulation (EC) No 1/2003.⁵⁷

2.2. General investigatory powers to collect information

In the domain of customs, tax (VAT) and GDPR enforcement, competent authorities in Italy enjoy broad investigative powers that can also encompass requests for electronic evidence to OSPs, but do not explicitly mention either category.

A similar consideration applies also with regard to information that might be stored abroad, especially if one considers that cooperation mechanisms in these areas are particularly efficient at the European Union level.

More specifically, both in customs and tax matters, enforcement powers are integrated in the EU dimension of customs control, and especially in the cooperation system circling OLAF investigations.⁵⁸ Since sharing data in this context, and more in general administrative cooperation, is reportedly rather successful,⁵⁹ obtaining information stored abroad usually does not require data acquisition from foreign OSPs directly by the national authorities. On the contrary, information is generally collected by the customs or tax authority of the interested Member State, thus avoiding the problem of potentially conflicting legal obligations for non-national private actors.

The integration of enforcement powers is also rather well developed in the GDPR domain (on which see below, Section 2.2.4). In this area too, requests for information regarding foreign OSPs are plausibly enforced, giving preference to the application of the local domestic law, to avoid conflicting legal obligations stemming from differences among legal systems.

2.2.1. Customs enforcement

In the area of customs enforcement, and especially in cases where undervaluation of goods is suspected, the ADM has the power to request information from economic operators that can assist in ascertaining the transaction value of goods. As the notion of “economic operator”, provided by the customs law, also at the EU level, is very broad,⁶⁰ it can also encompass OSPs.

⁵⁷ Article 15-*octies*, § 3, Law 287/1990.

⁵⁸ See e.g. ADM, *Rapporto di verifica* 2022, pp. 88 and followings, online <https://www.adm.gov.it/portale/documents/20182/535814/Rapporto+di+verifica+anno+2022.pdf/1c005c04-7ce6-4648-d0be-fc2992692abb?t=1688464393675>.

⁵⁹ In this sense, for instance, Tarini, (n. 8), pp. 44-45.

⁶⁰ See Article 5(5) and 48(2) Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code.

More specifically, the ADM may request data and documents relating to transport, insurance, freight and any other cost element forming the declared value for import, export, placing in customs or VAT warehouses and transit.⁶¹

In this regard, ADM has the authority to require information on the valuation of products (such as contracts, payments, financial arrangements, cost of transport and insurance, and expenses of deposits).⁶² Such requests may be addressed to importers, exporters, airport service companies, shipping companies, companies and natural persons engaged in the handling, storage, transport and customs representation of goods.

In addition, customs officers, for the purposes of reviewing the assessment, may also invite operators to provide information and documents concerning the goods which have been the subject of customs operations. In such cases, a time limit of not less than fifteen days is set in the request. Information and documents may also be requested from other public or private persons who appear to have been involved in the commercial transaction (thus, again, potentially including OSPs, although no specific mention is made in this regard).⁶³

The ADM's power to request information from private actors is not subject to any authorisation, and the collection and processing of data requested by the ADM shall be regarded as a processing of significant public interest under data protection law.⁶⁴

If information requests are not complied with, the ADM may impose a pecuniary penalty, ranging from a minimum of 5,000 euros to a maximum of 10,000 euros, in addition to the measures of suspension and revocation of the authorisations and faculties granted to non-compliant operators.⁶⁵ If the

⁶¹ See Article 40, § 3, Legislative Decree no. 141 of 26.09.2024 *Disposizioni nazionali complementari al codice doganale dell'Unione e revisione del sistema sanzionatorio in materia di accise e altre imposte indirette sulla produzione e sui consumi. (24G00156)* that replaced from September 2024 Article 35, § 35, Law Decree no. 223 of 04.07.2006, *Disposizioni urgenti per il rilancio economico e sociale, per il contenimento e la razionalizzazione della spesa pubblica, nonché interventi in materia di entrate e di contrasto all'evasione fiscale*, also in light of Article 140, Commission Implementing Regulation (EU) 2015/2447 of 24.11.2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code. Article 40, § 3, Legislative Decree 141/2024 confers ADM the use of the same powers – in this regard – provided for the investigation of VAT fraud (Article 51, Presidential Decree no. 633 of 26.10.1972 *Istituzione e disciplina dell'imposta sul valore aggiunto*).

⁶² See Tarini (n. 8), p. 39, reporting that 'officers commonly enforce this on a daily basis'.

⁶³ According to Article 11, § 2, Legislative Decree 374/1990.

⁶⁴ Article 53 of Legislative Decree no. 196/2003.

⁶⁵ See Article 51, no 2), Presidential Decree 633/1972.

information provided is false, the economic operator may also incur criminal liability.

2.2.2. Tax enforcement as regards VAT

To carry out their tasks in investigating VAT violations, the national legislation confers the competent authorities the power to (among others) order persons engaged in business, arts or professions, stating the reason, to produce documents and records, or to provide data, information and clarifications relevant to the assessment against them;⁶⁶ as well as to invite any person to produce or transmit, including photostatic copies, documents and invoices relating to certain supplies of goods or services received and to provide any information relating to such transactions.⁶⁷

Such requests for information are not subjected to particular conditions or authorisations. Moreover, they are provided in very broad terms, therefore they may be referred to also OSPs, though no mention of communications data or electronic data may be found in the law. An example of this occurrence emerges from a relatively recent development in the GDF's investigative techniques about domestic tax evasion, which could potentially be applied in VAT investigations too.

In some operations, evidence pertaining to tax evasion has been collected by examining social media posts, through collaboration with private companies (influencer marketing) and content hosted on adult platforms. Such information allowed the GDF to compare the actual income of the investigated persons and that reported in tax returns, noting inconsistencies.⁶⁸ To this aim, the GDF is currently developing programs to identify individuals whose position is characterised by the recurrence of one or more tax risks, also thanks to AI systems.⁶⁹ Specifically, the aim is to exploit interconnections with the databases at GDF's disposal, to identify risk criteria for functional auditing purposes and encourage spontaneous compliance.⁷⁰

⁶⁶ See Article 51, no 2), Presidential Decree 633/1972.

⁶⁷ See Article 51, no 4), Presidential Decree 633/1972.

⁶⁸ See, e.g., *IlSole24Ore*, 'Gdf recupera oltre 11 milioni di euro evasi da influencer. Tra loro Gianluca Vacchi e Luis Sal', 2024, online <https://www.ilsole24ore.com/art/prime-operazioni-gdf-agenzia-entrate-influencer-e-blogger-trovati-centinaia-migliaia-euro-sottratti-fisco-AFADGOzC>.

⁶⁹ In compliance with D.M. 28.06.2022 *del Ministero dell'Economia e delle finanze, attuativo delle nuove analisi di rischio basate sull'interconnessione fra le banche dati dell'Anagrafe tributaria di cui all'art. 1, comma 682, legge n. 160/2019 (legge di Bilancio 2020)*.

⁷⁰ The impact of such investigative techniques has already been brought to the attention of the Italian data protection authority (see § 2.3.4 below), that highlighted the risks for privacy protection, although with a partially positive assessment, see GPDP, *Valutazione di impatto*

Going back to the legislative provisions, non-cooperation with the requests of the authorities in the tax matter is a source of liability.⁷¹ In particular, the legislation punishes with an administrative sanction ranging from 1,000 to 8,000 euros any person who, during the inspections, refuses to produce or declares that they do not possess what is requested or in any case avoid the inspection and the verification of the documents, registers and records whose existence is certain, even if their retention is not compulsory.⁷² Similarly, the law punishes with an administrative sanction ranging from 250 to 2,000 euros the failure to comply with an invitation to appear and with any other request made by the competent authorities in the exercise of the powers conferred on them.⁷³ Moreover, legislative provisions also establish that, unless the act constitutes a more serious offence, a penalty of imprisonment from three to seven years shall be imposed upon whoever, to evade VAT, or to allow third parties to evade VAT, conceals or destroys all or part of the accounting records or documents whose retention is mandatory, so as not to allow the reconstruction of income or turnover.⁷⁴ Lastly, anyone who, in response to requests made by the authority,⁷⁵ produces or transmits deeds or documents that are false in whole or in part, or provides data and information that do not correspond to the truth shall be punished by means of criminal law.⁷⁶

sulla protezione dati relativa al trattamento “Analizzare rischi e fenomeni evasivi/elusivi tramite l'utilizzo dei dati contenuti nell'Archivio dei rapporti finanziari e l'incrocio degli stessi con le altre banche dati di cui dispone l'Agenzia delle entrate”.- Articolo 1, comma 684, della legge 27 dicembre 2019, n. 160 - 30 luglio 2022 [9808839], at: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9808839>.

⁷¹ No specific rules or remedies to protect the interests of the persons concerned by the financial tax requests are established under Italian law. Regardless of the affirmation of such rights in other sectors of the law (e.g. financial market law), a Supreme Court decision has recently downplayed the interpretation set forth by the European Court of Justice (ECJ) in the *DB* case (see below Section 2.2.3), relying on the nature of the real addressee of tax sanctions (a legal entity, not an individual), see Cass. civ., sez. trib., 01.03.2022, n. 6786, in *DeJure*.

⁷² Article 9, Legislative Decree 471/1997.

⁷³ Article 11, Legislative Decree 471/1997; see also Article 51, Presidential Decree 633/1972, referring to Article 32, §§ 3 and 4, d.P.R. n. 600/1973.

⁷⁴ Article 10, Legislative Decree 74/2000.

⁷⁵ And specifically in the exercise of the powers referred to in Articles 51 and 52 of Presidential Decree 633/1972.

⁷⁶ Pursuant to Article 76 of Presidential Decree no. 445 of 28.12.2000. The provision referred to in the first sentence, with regard to untrue data and information, shall apply only if, as a result of the requests referred to in the same sentence, the offences referred to in Legislative Decree no. 74 of 10.03.2000 are committed (see Article 11 Law Decree no. 201/2011). In such cases, penalties are increased from one third to one half, according to the discretion of the judge in the commensuration of punishment.

2.2.3. Punitive enforcement in the area of banking law and financial markets

The authorities competent in banking and financial market law enjoy general powers for requesting data. Although not specific for electronic evidence or OSPs, their broad mandate may encompass both.

Namely, in addition to what is illustrated above about the sole Consob (Section 2.1.1), TUB and TUF confer Banca d'Italia the power to carry out inspections at banks and entities to which they have outsourced corporate functions and request the production of documents and records that it deems necessary.⁷⁷ Much like Article 10 SSM R,⁷⁸ this provision could be interpreted as including also requests for electronic evidence. However, the remit of such requests (excluding financial data) appears somewhat limited in practice. In any case, the use of such investigative powers⁷⁹ is not subject to any specific conditions or authorisation, if performed to fulfil the supervisory functions entrusted to Banca d'Italia.

Against their investigative powers, both Banca d'Italia and Consob share some rules regarding the liability arising from their request to provide data.

Specifically, obstruction to their supervisory functions is sanctioned by several provisions. It is understood that such provisions also apply with regard to the investigative requests of the authorities; thus, also to requests to produce information, in principle including electronic evidence requested to OSPs.

Sanctions in case of lack of cooperation may be of criminal and administrative (punitive) nature. Under criminal law, the relevant provisions are Article 2638 of the Civil code and Article 170-*bis* TUF. Article 2638 c.c. deals with the obstruction to the exercise of the supervisory functions of Banca d'Italia or Consob.⁸⁰ This provision contains two offences, both punished by imprisonment.⁸¹ The first offence concerns the conduct of

⁷⁷ Article 54 TUB and Article 6-*bis* TUF.

⁷⁸ Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (SSM R).

⁷⁹ And in particular, those of Article 54 TUB and Article 6-*bis* TUF.

⁸⁰ The general reference to “supervisory functions” makes Article 2638 applicable also in regard to the ECB/SSM.

⁸¹ See, e.g., Cass. Sez. V, 22.02.2016, no. 6884. In case of companies with securities listed on regulated markets in Italy or in other EU Member States or widely distributed among the public, and penalties are doubled pursuant to Article 116 TUF. See, e.g., G. Messina, ‘Ostacolo all’esercizio delle funzioni delle autorità pubbliche di vigilanza’, in: G. Canzio, L. Domenico Cerqua and L. Luparia (eds.), *Diritto penale delle società, I, I profili sostanziali*

directors, general managers, executives responsible for preparing the corporate accounting documents, auditors and liquidators, and other persons subject by law to public supervisory authorities or with reporting duties towards the latter, which provide false information or fraudulently omit information bound to be submitted to the supervisory authority, with the purpose of obstructing its supervisory functions. The second offence contained in Article 2638 c.c. regards the conduct of the same subjects, which hinders the supervisory functions in any way, including omitting information that should be duly reported.⁸²

Apart from the cases covered by Article 2638 c.c., Article 170-*bis* TUF sanctions cases of obstructions of Banca d'Italia or Consob's supervisory functions with punishment up to two years imprisonment, in addition to a monetary fine ranging from 10,000 to 200,000 euros.

From an administrative point of view, non-cooperation with the authorities is sanctioned by Article 187-*quinqüesdecies* TUF. According to this provision, again apart from the cases covered by Article 2638 c.c., any person who (a) fails to comply with a request from Banca d'Italia or Consob within the prescribed time limits or (b) does not cooperate with the authority in the carrying out of its supervisory functions, or (c) delays the performance of such functions, shall be punished with the following sanctions. In case of a natural person, the applicable sanction ranges from 10,000 to 5 million euros; in case of a legal person, the sanction may amount to a fine of up to 5 million euros or, under certain conditions, up to 10% of the turnover. In case the advantage obtained is higher than the maximum penalty threshold established by law, penalties shall be determined in double the amount of such advantage.

Formally, the sanctions of Article 187-*quinqüesdecies* have an administrative nature. However, they have been recognised as substantially criminal by the Italian Supreme Court in light of the *Engel* criteria⁸³; the same interpretation was shared by the Italian Constitutional Court in a 2019 referral

(Padova; Wolters Kluvers/CEDAM, 2nd ed, 2016), pp. 553-591; V. Saponara, 'Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza', in: A. Cadoppi, S. Canestrari, A. Manna and M. Papa, *Diritto penale dell'economia*, Tomo I (Torino: UTET 2016), pp. 319-340; O. Capolino and R. D'Ambrosio, 'La tutela penale dell'attività di vigilanza', *Quaderni di Ricerca Giuridica della Consulenza legale, Banca d'Italia*, 2009, no. 67, pp. 20, 25.

⁸² With regard to Article 2638 c.c., it is worth noting that, according to some case-law, the possibility of triggering criminal liability under this provision should be excluded in cases of non-fraudulent lack of cooperation (e.g. mere omission), see Cass. Sez. V, 29.05.2019, no. 29377, related to the *Monte dei Paschi* scandal. Nonetheless, the wording of Article 2638 c.c. has not so far been amended by the legislature. Literally, this provision still includes both types of conducts (omissive and commissive).

⁸³ Cass., Sez. II civ., Ord. no. 3831 of 24.01.2018.

to the Court of Justice concerning the protection of the privilege against self-incrimination,⁸⁴ which was supported by the ECJ in the *DB* case.⁸⁵

2.2.4. GDPR enforcement

The GPDP's investigative powers in the domain of data protection enforcement are currently regulated by Article 58 of the GDPR and by GPDP's internal regulation, which coordinates with the GDPR.⁸⁶

According to the latter, the authority may order the data controller and processor, and, where applicable, the controller's or the processor's representative to provide any information it requires to perform its tasks. The GPDP may also obtain, from the controller and processor, access to all personal data and all information necessary for the performance of its functions; as well as get access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.⁸⁷ As further specified by the domestic regulation, in the course of an inspection, the GPDP may: (a) inspect, extract and acquire copies of documents, including in electronic format; (b) request information and explanations; (c) access databases and archives; and (d) acquire copies of databases and archives in electronic form.⁸⁸

Similar investigative powers are provided in case the GPDP investigates upon the reception of a complaint for a potential privacy breach.⁸⁹ In such circumstances, the GPDP shall examine the documentation received and may arrange for the acquisition of details and information concerning the facts and circumstances to which the complaint relates, including by hearing

⁸⁴ Ord. no. 117 of 10.05.2019 for the referral, and decision no. 84/2021 that implemented the ECJ decision in the Italian legal system.

⁸⁵ *DB v Commissione Nazionale per le Società e la Borsa (Consob)*, 02.02.2021, Case C-481/19, ECLI:EU:C:2021:84. The decision was followed by a further sentence by the Italian Constitutional Court - decision no. 84/2021 - that implemented the ECJ *dictat* in the Italian system. Following the ECtHR case-law (especially *Grande Stevens v. Italy*, 04.03.2014, no. 18640/10), the sanctioning procedures of both Banca d'Italia and Consob have been amended, to ensure a better compliance with fair trial rights also regarding remedies. In particular, the appeal procedure has been amended, providing affected individuals with the right to appeal the supervisors' decision before a judicial authority (namely, a civil court).

⁸⁶ Regulation no. 1 of 04.04.2019 *concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali* [9107633].

⁸⁷ See Article 58, § 1, let. a), e) and f) GDPR; see also Article 22, § 1, Regulation 1/2019.

⁸⁸ See Article 22, § 6, Regulation 1/2019.

⁸⁹ See Article 10, § 3, Regulation 1/2019.

in person or through an attorney the data controller or controller, by requesting information or the production of documents.⁹⁰

Providing false information to the GPDP is sanctioned by criminal law. In particular, unless the act constitutes a more serious offence, any person who, in proceedings or during investigations before the GPDP, falsely declares or attests information or circumstances or produces false deeds or documents shall be punished by imprisonment of from six months to three years.⁹¹ Moreover, persons who intentionally cause an interruption or disrupt the regularity of a proceeding before the authority or of the GPDP's inspections are punished with imprisonment of up to one year.⁹²

The requests for information issued by the GPDP, to carry out its particular tasks are not subject to any specific authorisation. Also, no specific rule or remedy is provided in domestic law to protect persons addressed by requests for information by the GPDP. This gap could be considered critical in light of the EU legislation, demanding that the 'exercise of the powers' listed in the same provision 'be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter'.⁹³

Besides this controversial aspect, the GPDP powers are clearly integrated in the EU dimension of privacy protection.⁹⁴

3. TRANSFER OF DATA BETWEEN PROCEEDINGS

In Italy, the specific regulation of administrative (punitive and non-punitive) proceedings results from the combination of a general, but rather basic legal framework,⁹⁵ with the sectoral regulation. The latter varies depending on the authority in charge and, at times, on the purpose of the

⁹⁰ Pursuant to Article 157 of the Privacy Code, as well as by proceeding pursuant to Article 2, Regulation 1/2019.

⁹¹ In accordance with Article 168 of the Italian Privacy Code.

⁹² More in general, non-compliance with the decisions of the GPDP (in particular, with the coercive powers of Article 58, § 2 GDPR) is also punished by Article 170 of the Italian Privacy Code, according to which '1. Whoever, not observing the measure adopted by the GPDP pursuant to Article 58(2)(f) of the Regulation, Article 2-septies(1), as well as the general measures referred to in Article 21(1) of the Legislative Decree implementing Article 13 of Law no. 163 of 25.10.2017, causes concrete harm to one or more data subjects shall be punished, on complaint by the injured party, with imprisonment from three months to two years'.

⁹³ Namely, Article 58, § 4 GDPR.

⁹⁴ As designed by Articles 60-61-62 GDPR.

⁹⁵ Composed essentially by Law no. 241 of 18.08.1990 and by the 'code of administrative proceedings', that is Law Decree no. 104 of 02.07.2010.

proceedings (especially considering that some authorities have a very broad competence, e.g. the customs authority).

Thus, the general law on administrative proceedings contains only very general minimum rules, upon which every public administration shall build its regulation.

Concerning evidence, it establishes that the administration responsible for the proceedings shall evaluate the admissibility of information used to issue a decision and may adopt all necessary acts and apply all measures to adequately perform its evaluations, including asking for oral statements, issuing production orders, and conducting inspections and other technical assessments.⁹⁶ In other words, each of the selected areas of administrative proceedings has, in principle, its own rules concerning the relationship with other administrative proceedings and with criminal justice authorities.

Also, in most cases, the sectorial rules provided for each administrative proceeding concern exchange of information, rather than transfer of evidence; from this, it follows that in many cases the transfer is meant to ‘simply’ provide criminal justice authorities with a *notitia criminis*. Nonetheless, information transferred from administrative to criminal law authorities may also take the form of documentary evidence. In this case, the admissibility issue arises (or may occur on a theoretical level, given that documentary evidence is admitted rather largely at trial).

The lack of a comprehensive legal framework also concerns voluntary forms of cooperation, for which no specific rules are established. The only exception stems from competition law, which explicitly provides a broad admissibility clause for all the elements collected by the AGCM.⁹⁷ Therefore, it could be argued that evidence obtained by voluntary cooperation should be admissible in competition law proceedings. In the other areas, given the broad discretion of competent authorities in exercising their investigative powers, it does seem plausible that information acquired *via* voluntary cooperation could be admissible in the sanctioning procedure. However, a practice in this sense, to obtain electronic evidence, has not been reported.

In line with such minimal requirements, the possibility to review the decision on admissibility is also relatively limited, due to the very broad margin of discretion granted to administrative authorities. Thus, unless otherwise provided, persons affected by the authorities’ powers may only challenge the final decision, according to the ordinary means of appeal established by the general provisions on administrative proceedings.

3.1. Transfers of data between national proceedings

⁹⁶ See Article 6(1), lit a) and b), Law Decree 104/2010.

⁹⁷ Article 12, § 1-*bis*, Law 287/1990.

Against this general background, the transfer of evidence among the administrative authorities illustrated in this study is only seldom regulated by legislative provisions. Exchange of information among such authorities is sometimes ensured by a series of Memoranda of Understanding. Although Memoranda do not directly tackle the issue of evidence admissibility, they *de facto* ensure a broad sharing of information among authorities, the most significant of which are reported below. This feature adds to the wide discretion granted to administrative authorities in considering all relevant elements to make their decisions.

More specifically, in competition law, when exercising its decision-making powers, the AGCM shall (in addition to the general legal framework⁹⁸) take into account all elements which it may already possess, or which are communicated to it by other public administrations or by everyone who might have an interest in the cause. The AGCM has also developed a series of Memoranda of Understanding with other independent supervisors (especially Banca d'Italia and Consob⁹⁹), which aim at facilitating the transfer of relevant information (without regulating in detail, however, the issue of admissibility criteria).

Concerning banking and financial markets law, none of the legislation regulating sanctioning procedures before Banca d'Italia or Consob provides for specific rules concerning admissibility among administrative proceedings.¹⁰⁰ Nonetheless, the two supervisory authorities have developed a series of Memoranda of understanding to facilitate the exchange of relevant information between them, in the various fields in which they exercise their competence.¹⁰¹

Conversely, general and systemic principles regulate the transfer of evidence from criminal to administrative proceedings.

Indeed, the requirements for admissibility of evidence are different and autonomous between administrative and criminal proceedings. Therefore, the status of a piece of evidence within a criminal trial is irrelevant for its potential admission in administrative proceedings. In such a context, only a few rules concern the transfer of evidence from a criminal to an administrative proceeding.

Firstly, the final decision issued within a criminal proceeding may become an evidentiary element (with the force of *res judicata*) in an

⁹⁸ According to Articles 12 and 14 of Law 287/1990.

⁹⁹ For the complete list, see <https://www.agcm.it/chi-siamo/normativa/protocolli-di-intesa?limit=0>.

¹⁰⁰ Including in that also Article 24, § 1 of Law no 262 of 28.12.2005, and by Law no. 681 of 24.11.1981.

¹⁰¹ A list of such agreements may be found at: <https://www.bancaditalia.it/compiti/vigilanza/accordi/accordi-consob/index.html>.

administrative proceeding, in accordance with Article 654 CCP. This value is recognised in respect of the defendant, the civil party and the civil liable party who has appeared or intervened in the criminal proceedings, when in such administrative proceedings a right or a legitimate interest whose recognition depends on the ascertainment of the same material facts that were the subject of the criminal proceedings is at issue (provided they have been deemed relevant to the criminal decision).

Secondly, transfer of evidence from criminal to administrative proceedings has to abide by the double-proportionality test established by the ECJ in its 2015 *WebMindLicences* decisions. However, no explicit rule has been introduced in the Italian legal system in this regard.¹⁰²

Lastly, in some sectoral legislation, rules have been provided that specify the exchange of information duties between criminal justice and administrative authorities. For instance, Article 187-*decies* TUF states that, when it becomes aware of one of the crimes related to market manipulation and insider trading, the prosecutor shall inform the Chairman of Consob without delay. And even where such violations do not constitute a criminal offence, Consob and the judicial authorities shall cooperate with each other, by exchanging information, to facilitate the detection of violations.¹⁰³ To this end, Consob may use the documents, data and information acquired by the Guardia di Finanza within the powers it can use for tax evasion investigations (also relating to VAT frauds).¹⁰⁴

A similar approach, grounded on the autonomy between administrative and criminal law, also characterises the transfer of evidence from administrative to criminal proceedings. Accordingly, the status of a piece of evidence within an administrative proceeding is irrelevant for its potential admission in a criminal trial. In the latter context, evidence shall be admitted only by applying the evidentiary rules provided by the criminal procedure code.¹⁰⁵

In this context, a general limit to the admissibility of information collected by administrative authorities is established by Article 220 of the rules implementing the Code of Criminal Procedure. According to this provision, if during inspections or supervisory tasks performed by

¹⁰² In this sense, however, S. Tesoriero, 'Indagini penali e amministrative in materia di frodi iva e doganali', in: A. Di Pietro and M. Caianiello (eds.), *Indagini penali e amministrative in materia di frodi IVA e doganali. L'impatto dell'European Investigation Order sulla cooperazione transnazionale*, Cacucci, 2016, pp. 17 and followings.

¹⁰³ See Article 187-*decies* TUF, §§ 1 and 3.

¹⁰⁴ See Article 63(1) of Presidential Decree no. 633 of 26.10.1972 and Article 33(3) of Presidential Decree no. 600 of 29.09.1973.

¹⁰⁵ For a brief recollection of the main rules in that context, see, e.g. M. Caianiello and G. Lasagni, 'Italy', in: F. Giuffrida and K. Ligeti (eds.), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, University of Luxembourg, 2019, pp. 171 and followings.

administrative authorities, suspicions of a crime emerge, then all the subsequent investigative acts shall be carried out in accordance with the rules of the criminal procedure code (and not the rules, usually less safeguarding, established for the administrative proceedings at stake).

Consequently, if evidence is collected according to standards other than those provided by criminal procedure law, after suspicions of a crime have emerged, such evidence shall not be deemed admissible in criminal proceedings. Nevertheless, as far as transfer of evidence is concerned, specific rules are often provided for in sectoral legislation, generally imposing a duty upon the administrative authority to refer potential *notitiae criminis* to the criminal justice authorities, if suspicions of a crime emerge during administrative proceedings.

In this regard, it is important to mention Article 331 CCP. According to it, public officials and persons in charge of public services have to report, without delay, any suspicions of crime arising in the course of carrying out, or because of their functions or service. This norm also applies to the personnel of the administrative authorities described in this report. At times, the sectoral legislation adds further requirements, sometimes as Memoranda of Understanding.

In particular, in customs and tax enforcement, while performing their duties, the ADM, the GDF and tax agency officials may assume the role of judicial police if suspicions of a crime emerge during their investigation. This status enables a direct collection of information within the domain of criminal investigations, limiting the issue of transfer of evidence.¹⁰⁶

In banking law, transfer of evidence from the Banca d'Italia to criminal justice authorities is regulated by Article 331 CCP and Article 7 TUB. According to Article 331 CPP, as already mentioned, public officials and persons in charge of public services have to report, without delay, any suspicions of crime arising in the course of carrying out, or because of their functions or service. Per Article 7, § 2 TUB, employees of the Banca d'Italia exercising their supervisory functions are to be considered public officials. Moreover, the professional secrecy generally applicable to the Banca d'Italia personnel cannot be opposed to judicial authorities when the information requested is necessary to investigate or prosecute criminal offences. However, the same provision also establishes that all irregularities detected, even when they might involve criminal offences, shall be reported by employees exclusively to the collegial managing body of the Banca d'Italia (*Direttorio*). This reporting duty refers to the information itself, as well as, in the most significant cases, where accuracy in the referral and effective cooperation

¹⁰⁶ See also Articles 20 and 21, Law Decree 74/2000 for the coordination between administrative and criminal proceedings in light of the *ne bis in idem* principle (substantial dimension).

between the Banca d'Italia and judicial authority are all the more necessary, to potential insights into the case, aimed at corroborating at a technical and legal level the relevance of the suspicions of a crime.

From the wording of Article 7, § 2 TUB, it is unclear whether this latter rule represents an exception to the general reporting duty established by Article 331 CPP. In particular, it is not clear whether the obligation to refer the *notitia criminis* to judicial authorities, which is exceptionally, not directly, applicable to public officials working for the Banca d'Italia, exists for the *Direttorio* of the Banca d'Italia. Although it would be appropriate to amend Article 7 TUB to clarify it, legal scholars (and, to a certain extent, also the Banca d'Italia itself) generally believe that the *Direttorio* remains indeed bound by duty to refer suspicions of crime to judicial authorities. The procedure of Article 7, § 2 TUB, therefore, shall be interpreted not as a real derogation to Article 331 CPP, but only as a precautionary reporting mechanism to prevent or reduce an unregulated dissemination of potential *notitiae criminis* having detrimental effects on the stability of the financial markets.¹⁰⁷

In financial markets law, transfer of evidence from Consob to criminal justice authorities is regulated by Articles 187-*decies* and followings TUF. According to Article 187-*decies*, § 2, the President of Consob shall transmit to the prosecutor the information collected during the administrative investigation, if evidence emerges suggesting the existence of a criminal offence. The transmission of the documents to the Prosecutor's Office shall take place *via* in a reasoned report and at the latest upon conclusion of the activity of ascertaining violations of the provisions by Consob.¹⁰⁸

¹⁰⁷ See L. F. Signorini, 'Attività di Vigilanza e Giurisdizione Penale', in: Associazione Italiana dei Professori di Diritto Penale. Il Convegno Nazionale – 'Economia e diritto penale nel tempo della crisi', Palermo 15.11.2013, p. 11, online www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2013/Signorini-151113.pdf (the author was, at the time, Vice-President of the Banca d'Italia); A. Antonucci, 'Articolo 7' in: C. Costa and A. Mirone (eds.), *Commento al Testo Unico delle Leggi in Materia Bancaria e Creditizia*, vol 1, Giappichelli 2013, pp. 58–59; G. Lasagni and I. Rodopoulos, 'A Comparative Study on Administrative and Criminal Enforcement of Banking Supervision at National Level', in: S. Allegrezza (ed.), *The Enforcement Dimension of the Single Supervisory Mechanism*, Milan, Italy, Wolters Kluwers, CEDAM, 2020, 608.

¹⁰⁸ The intensity of the relations between Consob and criminal proceedings is also shown by the power of the financial supervisor to exercise the rights and faculties attributed by the code of criminal procedure to the bodies and associations representing interests affected by the offence, within criminal proceedings for the crimes of insider trading and market manipulation. Consob may also file a civil action in the criminal proceedings, and request a reparation for the damage caused to the integrity of the market. Such sum shall be determined by the judge, also on an equitable basis, taking into account the offensiveness of the act, the

In competition law, in addition to the general norm of Article 331 CPP, the AGCM has entered into several Memoranda of Understanding with criminal investigating authorities (such as the GDF¹⁰⁹ or prosecution offices¹¹⁰), aiming at facilitating the transfer of information. Such Memoranda, however, do not specifically touch upon the issue of admissibility criteria.

Lastly, in privacy law, in addition to EU norms that regulate the transfer of information from privacy supervisors to the judicial authorities,¹¹¹ the Italian Privacy code, pursuant to Article 57, § 1, let. v) GDPR, explicitly requires the GPDP to denounce any fact that may constitute a criminal offence punishable *ex officio*, of which it becomes aware in the exercise or because of its functions.¹¹² Moreover, the authority has developed a series of Memoranda of understanding, to facilitate the exchange of relevant information with criminal justice authorities (the GDF, above all, but also prosecution offices), although without dwelling in details on aspects of evidence admissibility.¹¹³

personal qualities of the guilty party and the entity of the product or profit obtained from the offence (Article 187-*undecies* TUF).

Last, a specific rule also exists with regard to the application and enforcement of criminal and administrative sanctions in light of the substantial dimension of *ne bis in idem*. According to Article 187-*terdecies* TUF, when, for the same fact, a pecuniary administrative sanction or administrative sanction dependent on a crime or a criminal sanction has already been imposed, (a) the judicial authority or CONSOB shall take into account, when imposing the sanctions within its competence, the punitive measures already imposed; (b) the collection of the fine, the pecuniary sanction dependent on a criminal offence or the administrative pecuniary sanction is limited to the part exceeding that collected by the administrative authority or the judicial authority respectively.

¹⁰⁹ Of 05.04.2024, online https://www.agcm.it/dotcmsdoc/normative/Rinnovo_Protocollo_GDF-AGCM_05-04-2024.pdf.

¹¹⁰ See Protocollo d'intesa AGCM - Procura della Repubblica di Roma, 10.01.2018, online <https://www.agcm.it/chi-siamo/normativa/dettaglio?id=d094d24f-5e85-45a4-9242-55c16e39aade&parent=Protocolli%20di%20intesa&parentUrl=/chi-siamo/normativa/protocolli-di-intesa>; or Protocollo d'intesa AGCM - Procura della Repubblica di Milano, 11.01.2018, online <https://www.agcm.it/chi-siamo/normativa/dettaglio?id=a32f799c-f5c1-465f-be75-0819bcb72549&parent=Protocolli%20di%20intesa&parentUrl=/chi-siamo/normativa/protocolli-di-intesa>.

¹¹¹ See in particular, Article 33 GDPR.

¹¹² See Article 154, § 1, let d) Privacy Code.

¹¹³ A list of such agreements may be found at: <https://www.garanteprivacy.it/home/attivita-e-documenti/protocolli-d-intesa>.

3.2. Transfers of data between foreign and national proceedings

No general rules are provided under Italian law about the transfers of data between foreign and national proceedings. In general terms, however, and as anticipated (see above, Section 2.2), exchange of information is structurally part of the activity of some administrative authorities, which operate in a centralised or multi-level enforcement system. In this context, a further, very relevant, means of transnational transfer of evidence between administrative and criminal justice authorities is the OLAF cooperation system, which in Italy is successful in disseminating information that is later used as evidence in administrative proceedings.¹¹⁴

More specifically, on the one side, when data is to be transferred from foreign criminal to administrative proceedings, similarly to the case in which evidence is transferred from Italian criminal proceedings, administrative authorities enjoy a broad discretion in collecting relevant information and admitting it as evidence. This seems to be the approach also followed when criminal proceedings occur abroad.

Conversely, when data is to be transferred from a foreign administrative proceeding to a national proceeding, the speciality rule of criminal law applies. According to it, in criminal proceedings, evidence may be admitted only by using the evidentiary rules provided for by the criminal procedure code, which does not contain specific rules for cases where information derives from foreign administrative proceedings. Also in this case, the relevance of OLAF investigations brought to the development of a case-law by the Italian courts, especially with regard to the tax matter. According to it, no further investigation is generally required by national authorities following the transmission of OLAF final reports of the assessment contained in such reports. The latter are thus recognised as having the same evidentiary value as reports issued by national administrative authorities.¹¹⁵

4. CONCLUSION

In conclusion, the Italian system appears quite fragmented when it comes to enforcing administrative punitive sanctions.

Firstly, the recognition of the punitive nature of an administrative sanction is not defined by the law but left to the case-by-case approach of the jurisprudence. This confers a great flexibility to the legal framework, but – at the same time – makes it also somewhat uncertain to foresee the scope of the

¹¹⁴ On the admissibility of OLAF evidence in the Italian legal system, see M. Caianiello and G. Lasagni, (n. 105).

¹¹⁵ See M. Caianiello and G. Lasagni, (n. 105), pp. 176 and followings.

punitive matter in advance, and the adequacy of procedural and evidentiary law established in the legislation.

Secondly, the areas investigated in the present study are not homogeneous regarding the institutional framework of the competent authorities concerned. Although in most cases administrative sanctioning powers that might be considered punitive are enforced by administrative authorities, the latter vary in term of the independence they enjoy from the executive (independent in banking and financial market law, in competition law and about customs and privacy protection; under government control in the tax matters), as well as like their powers (strictly administrative under a formal perspective in banking, financial market, competition, and privacy law; hybrid of administrative and criminal in tax and custom law).

Thirdly, the domain of administrative proceedings, at least in the areas studied for the present research, does not present a common legal framework, but a multitude of sectoral regulations. No common rules, in this sense, exist concerning investigating powers, and transfer and admissibility of evidence.

Nonetheless, some common features may be noticed from a factual point of view. In particular, all the authorities involved *de facto* have in common a great degree of discretion in exercising their powers, which usually does not require external authorisations (though with some exceptions precisely when it comes to electronic communications). Accordingly, the transfer of information is characterised by a great flexibility, especially if compared with a criminal law perspective.

Against this background, the general lack of specific rules concerning both requests for information to OSPs and electronic evidence is not surprising. Still, the transversal character of digital information and of the providers that exercise control over it sheds a particularly critical light on both an efficient enforcement of sanctioning powers and a fair use of the information so collected within administrative or criminal proceedings. In this regard, a view to the European and comparative dimension, like the one carried out in the present study, may represent a first step towards simplifying and strengthening of procedural rules, which appears highly desirable in the current state.

10. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN LUXEMBOURG

S. LANNIER and S. TOSZA

1. COMPETENT AUTHORITIES IN SELECTED AREAS OF PUNITIVE ADMINISTRATIVE ENFORCEMENT¹

The five selected areas of punitive administrative law are enforced in Luxembourg by the following six authorities.

Customs enforcement is conducted by the Customs and Excise Administration (*Administration des Douanes et des Accises*, ADA). The ADA is under the authority of the Minister of Finance.² Its enforcement is mixed, as its agents can investigate violations of both administrative laws related to customs and excise obligations, and specific sectoral criminal offenses.³ When investigating criminal offenses, its agents act as judicial police officers and apply the Code of Criminal Procedure (*Code de procédure pénale*). For instance, its Article 67-1 provides the possibility to request phone and location data from online service providers (OSPs), and Article 66.8 to request information by electronic means. It should be mentioned that Luxembourg is part of the Belgo-Luxembourg economic union. As such, Luxembourg applies the Belgian General Law on Customs and Excise (GLCE). From a custom perspective, both countries are forming a unique

¹ The authors are grateful to all the professionals who shared their expertise and perspectives in the course of this research. Special thanks are due to Dr. Michel Erpelding for his insights on Luxembourgish administrative law, Dr. Fatima Chaouche, Dr. Julie Kaprielan and Dr. Arthur Bianco for their help with the Luxembourgish tax legislation, and Dr. Clémentine Boulanger for her support regarding data protection enforcement. All errors are our own.

² Article 2.1 of the Law Organising the ADA (*Loi du 27 juillet 1993 portant organisation de l'administration des douanes et accises*).

³ Law conferring New Powers and amending the Existing Powers of the ADA (*Loi du 27 juillet 1993 attribuant des compétences nouvelles et modifiant les compétences actuelles de l'administration des douanes et accises concernant la fiscalité indirecte et les attributions policières*); and Law empowering Customs Officials to exercise certain General Police Powers (*Loi du 9 juin 1994 ayant pour objet d'habiliter les agents de l'administration des douanes à exercer certaines attributions de la police générale*).

territory.⁴ Similarly, the European Union (EU) has created a unique customs territory.⁵ In practice, to ensure enforcement, the ADA requests mutual administrative assistance concerning entities established outside of Luxembourg.

Tax enforcement is mainly regulated under the general tax code.⁶ However, the 1979 Value Added Tax (VAT) Law⁷ creates an autonomous tax, which excludes the application of the general tax code. Such an exclusion has been criticised due to the many protective provisions under the general tax code that receive no equivalent in the VAT Law.⁸ VAT enforcement is conducted by the Registration, Domains and VAT Administration (*Administration de l'enregistrement, des domaines et de la TVA*, AEDT),⁹ which is under the authority of the Minister of Finance.¹⁰ Although the VAT Law provides for both administrative tax fines and criminal penalties, the AEDT can only issue tax fines, meaning that its enforcement is administrative.¹¹ In implementing its investigative powers, the AEDT is competent over the national territory:¹² its powers based on national law only regards persons residing or established in Luxembourg.¹³

The enforcement of administrative frameworks on banking and financial markets lies in two authorities: the Financial Sector Supervisory Commission (*Commission de Surveillance du Secteur Financier*, CSSF) and Insurances Commissariat (*Commissariat aux Assurances*, CAA). Both authorities have legal personality and financial autonomy and they are under the authority of the Minister responsible for these sectors.¹⁴ The nature of the enforcement of the CSSF is administrative as it can impose administrative

⁴ Articles 1 and 2 of the Convention establishing the Belgo-Luxembourg Economic Union (*Convention instituant l'Union économique belgo-luxembourgeoise*).

⁵ Article 4 of the Regulation (EU) no. 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code.

⁶ *Abgabenordnung*.

⁷ *Loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée*.

⁸ Legitech, 'TVA: Droit des assujettis', Articles LexNow, 18/07/2013.

⁹ The AEDT refused to participate to the research project.

¹⁰ Article 1.1.1.b of the AEDT Law (*Loi du 10 août 2018 portant organisation de l'Administration de l'enregistrement, des domaines et de la TVA, du recouvrement des impôts indirects*).

¹¹ Articles 77 to 80 of the VAT Law. Above certain amounts, specific administrative offenses automatically become criminal offenses and thus lies in the jurisdiction of courts only.

¹² Article 14.1 of the AEDT Law.

¹³ P. Mellina, 'Acteurs et déclenchement du contrôle TVA au Luxembourg', *Cahiers de fiscalité luxembourgeoise et européenne*, 2024, vol. 2024/2, p. 108.

¹⁴ Article 1.1 of the Law creating the CSSF (*Loi du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier*) and article 1.1 of the Insurance Sector Law (*Loi du 7 décembre 2015 sur le secteur des assurances*).

sanctions.¹⁵ It is interpreted by the literature as the ‘economic administrative police’.¹⁶ The European Court of Justice (ECJ) also considers as administrative the enforcement by similar national authorities.¹⁷ However, the literature questioned the nature of the enforcement by the CSSF, particularly in light of the case law of the European Court of Human Rights (ECtHR).¹⁸ In view of the level of fines that can be adopted by the CSSF, the literature considers that its enforcement can qualify as criminal.¹⁹ Similarly, the administrative court declared that an administrative sanction proceeding ‘is similar to criminal proceedings’.²⁰ As the CAA can only impose administrative fines, the nature of its enforcement is administrative.²¹

Enforcement of competition law is conducted by the Competition Authority (*Autorité de la concurrence*). It is an independent administrative authority with legal personality,²² which can adopt administrative sanctions. Hence, its enforcement is administrative.

Finally, the regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) is enforced by the National Commission for Data Protection (*Commission nationale pour la protection des données*, CNPD),²³ an independent public entity with legal personality.²⁴ As the CNPD can only issue administrative sanctions,²⁵ its enforcement is administrative by nature. However, due to the seriousness of these sanctions, part of the literature considers that the GDPR enforcement by competent authorities should

¹⁵ See, for instance, articles 63 and followings of the Law on the Financial Sector (*Loi du 5 avril 1993 relative au secteur financier*).

¹⁶ M. Limpach, F. Goergen, ‘Les compétences, pouvoirs et moyens d’intervention de la CSSF’, in: Association luxembourgeoise des juristes de droit bancaire (ed.), *Droit bancaire et financier au Luxembourg 2014: recueil de doctrine*, Larcier ; Anthemis, Hors collection Larcier, 2014, p. 165.

¹⁷ ECJ, *UBS Europe SE and Alain Hondequin and Others v. DV and Others*, 13.09.2018, C-358/16, §§ 41-47.

¹⁸ ECtHR, *Engel and Others v. the Netherlands*, 08.06.1976, no. 48272/17, 57479/17, 510/18, 7936/18, 27115/18.

¹⁹ Limpach, Goergen, (n. 16), p. 217; A. Lutgen, M. Marty, ‘La pratique des sanctions administratives en matière financière’, *Journal des tribunaux Luxembourg*, Larcier, 2017, vol. 2, no. 50, p. 52.

²⁰ Cour administrative, 16.12.2014, no. 34766C, p. 9.

²¹ See, for instance, Article 303 and followings of the Insurance Sector Law.

²² Articles 6.1 and 7 of the Competition Law (*Loi du 30 novembre 2022 relative à la concurrence*).

²³ The CNPD refused to participate to the research project.

²⁴ Article 3 of the Law organising the CNPD (*Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données*).

²⁵ Article 48 of the Law organising the CNPD.

qualify as criminal.²⁶ The CNPD is competent to exercise its powers on the territory of Luxembourg.²⁷

2. PUNITIVE ADMINISTRATIVE PROCEEDINGS: GENERAL FRAMEWORK

The general framework on administrative proceedings is rather limited in Luxembourg. The Law of 1978 governing the Non-Contentious Administrative Procedure (henceforth, the Law of 1978)²⁸ and Grand-Ducal Regulation of 1979 on Non-Contentious Administrative Procedure (henceforth, Regulation on Non-Contentious Administrative Procedure)²⁹ are applicable whenever sectoral laws do not consider at least equivalent guarantees³⁰ and regulate the procedure to elaborate an administrative individual decision.³¹ These texts are also to be applied even by civil courts when those are competent, for instance, on VAT enforcement.³² Yet, the applicability of the Law of 1978 to VAT proceedings is still being discussed by courts.³³

However, the guarantees and remedies provided by this framework might not be applicable to request for data to OSPs by administrative authorities, given the nature of these requests. Indeed, remedies and guarantees are in general available against administrative individual decisions.³⁴ However, the preparatory acts do not qualify as administrative decisions. As a result, the case law interpreted requests for data (when no sanction is mentioned) as not amounting to an individual decision, in that case, in the field of competition enforcement. A decision to realise a control or to request information are qualified as mere steps of the investigation and not as final administrative decision.³⁵ Hence, many safeguards against

²⁶ O. Tambou, J.F. López Aguilar, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, Droit administratif, 2020, ¶ 418.

²⁷ Articles 55.1 and 57.1.h of the GDPR.

²⁸ *Loi du 1er décembre 1978 réglant la procédure administrative non contentieuse*. The law aims at implementing Committee of Ministers, *Resolution (77) 31 on protection of the individual in relation to the acts of administrative authorities*, Council of Europe, 28/09/1977.

²⁹ *Règlement grand-ducal du 8 juin 1979 relatif à la procédure à suivre par les administrations relevant de l'Etat et des communes*.

³⁰ Article 4 of the Law on Non-Contentious Administrative Procedure.

³¹ P. Schmit, *La protection de l'administré dans le cadre de la procédure administrative*, Conseil d'Etat, 2015, p. 39.

³² Cour de cassation, 17.10.2012, no. 55/2012.

³³ O. Coulon, 'Les sources du contrôle TVA', *Cahiers de fiscalité luxembourgeoise et européenne*, 2024, vol. 2024/2, pp. 90-93.

³⁴ Schmit, (n. 31), pp. 15-20.

³⁵ Tribunal administratif, 28.05.2018, no. 38364, 39127, 39876.

individual decisions might not be available to requests for data to OSPs, unless a decision imposing a sanction is adopted.

2.1. Framework on non-contentious administrative procedure

The Law of 1978 and the Regulation on Non-Contentious Administrative Procedure are relevant to the gathering of data by administrative authorities from OSPs as it sets basic guarantees and rights for any person concerned by an administrative proceeding and potential third parties involved in such proceeding. Article 1 of the Law of 1978 mandates the regulation to provide rules to implement the rights of defence and the adversary principle. These include the right to be heard when an administration prepares a decision independently of the initiative of the concerned person, such as a sanction against an OSP. It requires that, unless such delay would jeopardise the investigation, the administration informs by mail ‘the party concerned of its intention by communicating the factual and legal grounds for its action’.³⁶ The person has then eight days to present any observation and can request to be heard. The case law assessed, particularly regarding CSSF’s decisions, that administrative authorities cannot refer in general to this provision and should explicitly mention to the person their right to be heard.³⁷ However, an administrative decision can be annulled due to a violation of the right to be heard only if the hearing of the person, for instance an OSP fined for not providing data for a technical impossibility, would have led to a different outcome.³⁸ The rights of defence also mandate the administration to notify the concerned person of their right to be assisted by a legal or technical counsellor.³⁹

The adversary principle translates into a right to obtain access to the administrative file.⁴⁰ The access to certain documents can be refused due to important public or private interests, or in case of emergency, but a document the inspection of which has been refused to a party may only be used to their

³⁶ Article 9 of the Regulation on Non-Contentious Administrative Procedure.

³⁷ Cour administrative, 03.05.2022, no. 46817C. Decision commented by P. Schmit, ‘Procédure administrative non-contentieuse : la Cour administrative sanctionne de nullité la non-information de l’administré sur son droit de demander à être entendu en personne Cour administrative, 3 mai 2022’, *Revue luxembourgeoise de droit public*, 2023, vol. 15/2023, p. 170; M. Mathieu, S. Minette, ‘Les garanties procédurales encadrant le pouvoir de sanction de la CSSF’, in: N. Thieltgen (ed.), *Droit bancaire et financier au Luxembourg 2024 Vol. I Évolution législative – Cadre légal et réglementaire*, Larcier-Intersentia, Hors collection Larcier, 1st ed., 2024, pp. 456-458.

³⁸ Cour administrative, 03.05.2014, no. 34051C.

³⁹ Article 10 of the Regulation on Non-Contentious Administrative Procedure. This provision must be interpreted along the Law on Transparent and Open Administration (*Loi du 14 septembre 2018 relative à une administration transparente et ouverte*).

⁴⁰ Cour administrative, 03.10.2002, no. 14687C.

disadvantage if the authority has previously communicated to them in writing the essential content relating to the case and given them the opportunity to submit their observations.⁴¹ However, this limitation of access must be considered an exception and as such be applied restrictively.⁴² The case law interpreted that the communication of the administrative file has to ‘necessarily include the factual elements and documents that may be relevant to the exercise of the authority’s jurisdiction over the person concerned and the decision actually envisaged’.⁴³ Therefore, it is not an ‘unlimited and absolute right of access to all information processed by the competent authority as part of its investigation’, as the administration can exclude elements that are not relevant to the specific case.⁴⁴ A person concerned may seek remedy against a decision not to provide elements, which that person considered to be relevant.⁴⁵

The legality of an administrative decision depends on the validity of its motive,⁴⁶ which can be supplemented during appeals if insufficient.⁴⁷ While formal motivation is required for certain decisions,⁴⁸ such as the outcome of an administrative remedy against a coercive fine to mandate an OSPs to provide data, the request for data, *per se*, does not seem to have to be explicitly motivated. The lack of motivation, when mandatory, will suspend the remedies’ delays.⁴⁹

This framework offers basic rules on remedies open to affected persons and third parties against the implementation of the powers of administrative authorities. Indeed, the Regulation on Non-Contentious Administrative Procedure provides for administrative remedies whenever a law does not consider them. These remedies are threefold: firstly, the persons concerned by an administrative decision can request the decision to be reassessed by the same authority who adopted it (e.g., the investigator); secondly, they can request its reassessment by the hierarchical superior of the authority (e.g., the director); thirdly, they can file a remedy at the supervising authority, which

⁴¹ Article 13 of the Regulation on Non-Contentious Administrative Procedure.

⁴² Cour administrative, 27.06.2017, no. 39457C.

⁴³ Cour administrative, 17.12.2019, no. 42666C, p. 12. Decision commented by M. Trienbach, ‘Procédure administrative non contentieuse et accès au dossier dans une procédure de sanction administrative’, *Revue luxembourgeoise de droit public*, 2021, vol. 9/2021, pp. 47-48.

⁴⁴ Mathieu, Minette, (n. 37), p. 452.

⁴⁵ Cour administrative, (n. 43), p. 12. The judge will decide on this case based on the balancing test from ECJ, (n. 17).

⁴⁶ Conseil d’Etat, *Deutsche Buchgemeinschaft*, 11.03.1970, *Pasicrisie luxembourgeoise – Recueil Trimestriel de la Jurisprudence Luxembourgeoise*, vol. 1969-1971/1a, pp. 339-347; Cour administrative, 09.02.1999, no. 11084C.

⁴⁷ Cour administrative, 20.10.2009, no. 25738C.

⁴⁸ Article 6 of the Regulation on Non-Contentious Administrative Procedure.

⁴⁹ Cour administrative, 08.07.1997, no. 9918C.

will only verify the legality of the decision (e.g., the ministry).⁵⁰ The absence of an answer to any of those requests within three months is to be understood as a negative answer.⁵¹ In parallel to administrative remedies, a complaint can be filed to the Ombudsman.⁵² Against the administrative decision(s) resulting from the previous administrative remedies, further remedies are open to the administrative tribunal.⁵³

These remedies are open to third parties, meaning, to persons who are not the addressees of the administrative decision, whenever they have a personal, direct and legitimate interest to file a complaint.⁵⁴ For instance, the investigated person could file a complaint against a sanction decision adopted against an OSP refusing to provide data to an administration, on the basis that such data is protected by professional secrecy.

2.2. General principles of administrative law

Some general principles of administrative law identified by administrative courts remain uncoded but apply as core values essential to the legal system.⁵⁵ Firstly, the decision power of administrative authorities must be implemented impartially. Secondly, authorities must act and decide within a reasonable delay. Such a delay includes the timeframe of the investigation, assessed by courts, balanced with the need for a detailed investigation to obtain a proportional and adequate outcome.⁵⁶ Finally, the principle of proportionality is recognised as a constitutional principle,⁵⁷ which requires administrative authorities to balance between individual rights and the objective of public interest of the investigation or decision.

⁵⁰ Article 6 of the Regulation on Non-Contentious Administrative Procedure, detailed by the case law, Schmit, (n. 31), pp. 59-70.

⁵¹ Article 13.3 of the Law on the Rules of Procedure before the Administrative Courts.

⁵² Law establishing an Ombudsman (*Loi du 22 août 2003 instituant un Ombudsman*).

⁵³ Articles 2 and 3 of the Law on the Organisation of Administrative Courts (*Loi du 7 novembre 1996 portant organisation des juridictions de l'ordre administrative*).

⁵⁴ Articles 5 and 12 of the Regulation on Non-Contentious Administrative Procedure.

⁵⁵ Cour constitutionnelle, 22.01.2021, no. 152/21. Commented by Mathieu, Minette, (n. 37), pp. 463 and followings.

⁵⁶ Cour administrative, 08.12.2022, no. 47780C.

⁵⁷ Cour constitutionnelle, 19.03.2021, no. 146/21; A. Klethi, 'Le principe de proportionnalité à la lumière de la jurisprudence de la Cour constitutionnelle et des juridictions administratives luxembourgeoises', *Revue luxembourgeoise de droit public*, 2023, vol. 15/2023, p. 145.

3. PUNITIVE ADMINISTRATIVE PROCEEDINGS: SECTORAL FRAMEWORK

3.1. Requests for data to online service providers

Specific legal bases to request certain data to certain OSPs rely on categories transposed from EU law. Those laws refer to providers of electronic communication services and public communication networks operators, as for example in the Law on the Electronic Communications Sector.⁵⁸ Operators provide transmission systems and, ‘where applicable, switching or routing equipment and other resources [...] which permit the conveyance of signals’, used wholly or mainly for the provision of publicly available electronic communications services.⁵⁹ Providers deliver those electronic communications services, meaning ‘a service normally provided for remuneration which consists wholly or mainly in the transmission of signals over electronic communications networks’.⁶⁰ This provision transposes only partially Article 2.4 of the European Electronic Communications Code, as there is no mention of internet access services and interpersonal communication services.

For these requests, legal bases mention the obtaining of traffic data. This category was defined under the national law before the adoption of the Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (European Production Order Regulation), and those definitions are not aligned. It relates to ‘all data processed for the purpose of routing a communication via an electronic communications network or for billing purposes’,⁶¹ and it is distinguished from location data.⁶²

3.1.1. Customs enforcement

No specific legal basis exists for the ADA to request data from OSPs. However, the ADA has a general power to request any information deemed

⁵⁸ *Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l’égard du traitement des données à caractère personnel dans le secteur des communications électroniques.*

⁵⁹ Article 2.h.2 and i.2 of the Law on the Electronic Communications Sector. This definition transposes Article 2.1 of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

⁶⁰ Article 2.j.2 of the Law on the Electronic Communications Sector.

⁶¹ Article 2.e.2 of the Law on the Electronic Communications Sector.

⁶² Article 2.f.2 of the Law on the Electronic Communications Sector.

necessary.⁶³ Aside the concerned persons, meaning, importers and exporters, the ADA can request information from ‘all persons directly or indirectly involved in the import or export of goods’, which could, potentially, include OSPs.⁶⁴

The administration can specifically request ‘invoices, bills, copies of letters, cash books, inventory books and all books, registers, documents and correspondence relating to their commercial or professional activity’, and generally any ‘documents and correspondence that establish or help to establish a customs or excise offence’, which could include electronic information. The transfer of information must be done by mail or electronically. Electronic documents should be provided ‘in a legible and intelligible form’,⁶⁵ and the ADA can request to receive their copy in a specific form.⁶⁶ The owner of the retained documents should receive a list of those documents. Refusal to comply with the request can be punished by a fine between 25 to 250 euros.⁶⁷

Once a request for documents qualifies as a decision with legal effects for one of various persons,⁶⁸ any person who is directly and individually affected, such as an OSP fined for not answering to a preliminary request, or the concerned person, has an administrative redress against the decision.⁶⁹ Such a remedy must be motivated and filed, in general, within the three months after the third open day after the sending of the decision.⁷⁰ The GLCE details the right to be heard during the redress proceedings.⁷¹ Before adopting an unfavourable decision, the ADA must communicate its motivation by writing and the affected person has then thirty days to communicate their point of view by writing. When adopting the decision, the ADA must justify its divergence with the affected person. The affected person can request to be heard again. The final decision is notified to the affected person.⁷²

3.1.2. Tax enforcement as regards VAT

The AEDT has no specific investigative power to request data from OSPs. Yet, the power to obtain data from third parties is particularly relevant

⁶³ Article 203 of the GLCE (*Loi générale du 18 juillet 1977 sur les douanes et accises*), similarly provided at Article 15 of the Union Customs Code.

⁶⁴ When requests are directed to credit institutions, bankers and stockbrokers, the request must be previously authorised by the director of the ADA.

⁶⁵ Article 230.1 in relation with Article 201.2 of the GLCE.

⁶⁶ Article 230.2 of the GLCE.

⁶⁷ Article 230.3 of the GLCE.

⁶⁸ Article 211 of the GLCE.

⁶⁹ Articles 211 and 212 of the GLCE.

⁷⁰ Article 213 of the GLCE.

⁷¹ Articles 212/1 and 217 of the GLCE.

⁷² Article 219 of the GLCE.

as ‘it enables the AEDT to cross-check taxpayers’ declarations with data supplied by third parties’.⁷³ Therefore, the AEDT can generally gather information from any person⁷⁴ under Article 70 of the VAT Law, whenever it is necessary to detect tax infringements and to verify their correct collection.⁷⁵ The AEDT can request from any person ‘documents and invoices received at the time of delivery of goods or provision of services and [...] all information relating to these operations’,⁷⁶ which can include information stored electronically. Additionally, any VAT taxpayer – even the one who is not being investigated – must provide ‘all books, journals and accounting records, receipts, bank statements, purchase orders and shipping and transport documents’.⁷⁷ Warehouse or logistics platform for storing goods for delivery and payment service providers receive additional obligations to retain and transmit information.⁷⁸ In practice, it seems that the AEDT is regularly requesting data from taxpayers, but it remains rare that it requests ‘any person’.⁷⁹

In principle, information and documents must be consulted on site.⁸⁰ However, when documents exist in an electronic format, they must be transferred by mail or any other way decided by the AEDT, potentially, electronically. If the amount of data or the weight of the files so requires, the AEDT can provide a one-time exchange platform to share the requested information. Yet, it seems that this platform is not properly working in practice, leading to most documents being sent by email or post, or through both channels.⁸¹ Furthermore, such data must be legible and intelligible, as well as conform with the original.⁸² No deadline is set by law, leading to diversified practice of the AEDT’s agents, between one week to more than a month.⁸³ The absence of answer to a request for information qualifies for a

⁷³ Mellina, (n. 13), p. 100.

⁷⁴ By exception, due to the banking secrecy, financial institutions cannot provide individual information on their clients and on accounts, articles 1 and 2 of the regulation on banking secrecy (*Règlement grand-ducal du 24 mars 1989 précisant le secret bancaire en matière fiscale et délimitant le droit d’investigation des administrations fiscales*). The literature also considers that the AEDT must respect the legal professional privilege, *Ibid.* p. 109.

⁷⁵ Article 70.1§1 of the VAT Law.

⁷⁶ Article 70.1§1 of the VAT Law.

⁷⁷ Article 70.1§2 of the VAT Law.

⁷⁸ Articles 70*bis* and 70*ter* of the VAT Law.

⁷⁹ M. Lambion, ‘Le déroulement du contrôle. TVA Pouvoirs de contrôle de l’AEDT et analyse de la pratique administrative du contrôle’, *Cahiers de fiscalité luxembourgeoise et européenne*, 2024, vol. 2024/2, p. 128.

⁸⁰ Article 70.1§3 of the VAT Law.

⁸¹ Lambion, (n. 79), p. 129.

⁸² Article 70.3 of the VAT Law.

⁸³ Lambion, (n. 79), p. 130.

tax fine of 250 to 10.000 EUR,⁸⁴ or 10 to 50 per cent of the VAT evaded or refund unduly obtained.⁸⁵ The director of the AEDT can also decide on a daily fine of up to 25.000 euros, from the date set in their decision – and not from the date of the request for information.⁸⁶

A remedy exists only for OSPs against a decision imposing a sanction, hence if no sanction was imposed, there is no formal way of questioning a decision of the AEDT to request data.⁸⁷ If applicable, the taxpayer will be notified of any outcome of the investigation, which can be challenged through a complaint to civil courts.⁸⁸ The complaint of the taxpayer should be duly motivated,⁸⁹ which interpretation has enabled, in some cases, to limit access to remedies.⁹⁰ Yet, the possibility for the AEDT to reject a complaint due to not being ‘duly’ motivated is currently being debated by courts, as well as it is widely criticised by the literature as it creates a heavy evidence burden on the taxpayer.⁹¹ In case of a judicial complaint, there is a lack of clarity regarding its addressee due to the lack of legal personality of the AEDT. Despite this situation, most of the case law designated the AEDT as the addressee of both the notification and the subpoena.⁹² Yet, legal insecurity remains on that topic.⁹³

A study of tax controls by the AEDT further highlighted practical issues regarding remedies for taxpayers, deriving from legal gaps. Firstly, at the beginning of the control, very few taxpayers receive information about their rights, such as concerning legal assistance, on the consequences of a refusal to provide information, on the right to not self-incriminate oneself, or on the potential transfer of such information to other administrations or to judicial

⁸⁴ Article 77.1 of the VAT Law.

⁸⁵ Article 77.3 of the VAT Law.

⁸⁶ Article 77.2 of the VAT Law.

⁸⁷ Article 79 of the VAT Law.

⁸⁸ See, for instance, Articles 55.9 and 10, 67-3, 76.2, and 79 of the VAT Law.

⁸⁹ Article 76.3 of the VAT Law.

⁹⁰ J. Kaprielian, ‘Droit au recours effectif de l’assujetti et caractère dûment motivé de la réclamation en matière de TVA : une conciliation délicate clarifiée par le tribunal d’arrondissement’, *Cahiers de fiscalité luxembourgeoise et européenne*, 2023, vol. 2023/2, pp. 259-264.

⁹¹ M.-I. Richardin, L. Griffon, ‘L’exigence d’une réclamation dûment motivée en matière de TVA mise à mal par le juge luxembourgeois’, *Revue générale de fiscalité luxembourgeoise*, 2024, vol. 2024/2, p. 60; J. Kaprielian, ‘La protection effective de l’assujetti et le contrôle TVA’, *Cahiers de fiscalité luxembourgeoise et européenne*, 2024, vol. 2024/2, pp. 192-193; O. Coulon, ‘La clôture du contrôle fiscal’, *Cahiers de fiscalité luxembourgeoise et européenne*, 2024, vol. 2024/2, pp. 238-239.

⁹² T. Hoscheit, ‘Les instances dirigées contre l’Administration de l’enregistrement, des domaines et de la TVA : chronique d’un désastre judiciaire’, *Revue des procédures*, 2020, vol. 1/2020, p. 44. Recently, see Cour d’appel, 30.10.2024, no. 131/24.

⁹³ Coulon, (n. 91), pp. 241-242.

authorities.⁹⁴ Secondly, records of the proceedings are drafted by the AEDT and do not have to be discussed previously with the addressee.⁹⁵ The latter problem is criticised for bringing evidence *a posteriori*, which cannot be then contested.⁹⁶ Furthermore, these records are often lengthy and complex to understand, and they usually do not discuss the elements discussed by the taxpayer. The legal motivation of a decision is often only provided in the director's decision or during judicial proceedings.⁹⁷ Additionally, some taxpayers do not receive any records, and even are denied by the AEDT to access them.⁹⁸ Thirdly, when the control does not lead to a fine, the taxpayer is not always notified of the end of the control.⁹⁹ When the addressee of a decision is notified, the AEDT merely has to post the letter, independently of its effective receipt.¹⁰⁰ Independently of the outcome of the control, it remains provisional, enabling the AEDT to control again at a later stage, as long as the taxpayer's obligations are not prescribed.¹⁰¹ Finally, when the director decides on a fine, no prior discussion with the addressee of the fine is provided for.¹⁰²

3.1.3. Punitive enforcement in the area of banking law and financial markets

The core of enforcement powers of the CSSF lies in the Law on the Financial Sector. Enforcement powers of the CAA are regulated by the Insurance Sector Law. Additional powers of investigation are granted to the CSSF and the CAA by special sectoral laws. The CSSF receives additional legal bases for administrative investigations under 18 laws, including from the Law on Payment Services,¹⁰³ the Law on Undertakings for Collective Investment (UCI),¹⁰⁴ the Law on Alternative Investment Fund Managers (AIFM),¹⁰⁵ the Law on Market Abuse,¹⁰⁶ or the Law on Markets in Financial

⁹⁴ Kaprielian, (n. 91), pp. 174-176.

⁹⁵ Article 68 of the VAT Law.

⁹⁶ Lambion, (n. 79), p. 125.

⁹⁷ Kaprielian, (n. 91), pp. 178, 188.

⁹⁸ *Ibid.* p. 179.

⁹⁹ Lambion, (n. 79), p. 141.

¹⁰⁰ Coulon, (n. 91), p. 224.

¹⁰¹ *Ibid.* pp. 219-221, 226-228.

¹⁰² Coulon, (n. 91), p. 215.

¹⁰³ *Loi du 10 novembre 2009 relative aux services de paiement à l'activité d'établissement de monnaie électronique et au caractère définitif du règlement dans les systèmes de paiement et les systèmes de règlement des opérations sur titres.*

¹⁰⁴ *Loi du 17 décembre 2010 concernant les organismes de placement collectif.*

¹⁰⁵ *Loi du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs.*

¹⁰⁶ *Loi du 23 décembre 2016 relative aux abus de marché.*

Instruments.^{107,108} Powers under the following laws are common to both authorities: Law on OTC Derivatives, Central Counterparties and Trade Repositories (Law on OTCD),¹⁰⁹ Law on Key Information Documents for Packaged Retail and Insurance-Based Investment Products (Law on KID),¹¹⁰ Law on Indices,¹¹¹ Law on the Operationalisation of European Regulations in the Area of Financial Services,¹¹² Law establishing a Register of Fiducies and Trusts,¹¹³ and Law on Inactive Accounts, Inactive Safe-Deposit Boxes and Unclaimed Insurance Contracts (Law on Inactive Accounts).¹¹⁴ This diversity of texts results in a lack of harmonisation of investigatory powers, complicating the interpretation of whether they refer to distinct powers or should instead be understood as equivalent.

¹⁰⁷ *Loi du 30 mai 2018 relative aux marchés d'instruments financiers.*

¹⁰⁸ As well as from: Law on Investment Companies in Risk Capital (*Loi du 15 juin 2004 relative à la société d'investissement en capital à risque*), Law on Institutions for Occupational Retirement Provision (*Loi du 13 juillet 2005 relative aux institutions de retraite professionnelle sous forme de SEPCAV et ASSEP*, Law on institutions for occupational retirement provision), Law on Specialised Investment Funds (*Loi du 13 février 2007 relative aux fonds d'investissement spécialisés*), Law on Transparency Requirements (*Loi du 11 janvier 2008 relative aux obligations de transparence des émetteurs*), Law on Mandatory Squeeze-Out and Sell-Out of Securities (*Loi du 21 juillet 2012 relative au retrait obligatoire et au rachat obligatoire de titres de sociétés admis ou ayant été admis à la négociation sur un marché réglementé ou ayant fait l'objet d'une offre au public*), Law on Short Selling of Financial Instruments (*Loi du 12 juillet 2013 relative à la vente à découvert d'instruments financiers*), Law concerning the Audit Profession (*Loi du 23 juillet 2016 relative à la profession de l'audit*), Law on Payment Accounts (*Loi du 13 juin 2017 relative aux comptes de paiement*), Law implementing Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on Interchange Fees for Card-Based Payment Transactions (*Loi du 27 février 2018 relative aux commissions d'interchange et modifiant différentes lois relatives aux services financiers*, Law implementing Regulation 2015/751), Law on Central Securities Depositories (*Loi du 6 juin 2018 relative aux dépositaires centraux de titres*), Law on Prospectuses for Securities (*Loi du 16 juillet 2019 relative aux prospectus pour valeurs mobilières*), Law establishing an IBAN Central Electronic Data Retrieval System (*Loi du 25 mars 2020 instituant un système électronique central de recherche de données concernant des comptes IBAN et des coffres-forts*), and Law relating to the Issue of Covered Bonds (*Loi du 8 décembre 2021 relative à l'émission de lettres de gage*).

¹⁰⁹ *Loi du 15 mars 2016 relative aux produits dérivés de gré à gré, aux contreparties centrales et aux référentiels centraux et modifiant différentes lois relatives aux services financiers.*

¹¹⁰ *Loi du 17 avril 2018 relative aux documents d'informations clés relatifs aux produits d'investissement packagés de détail et fondés sur l'assurance.*

¹¹¹ *Loi du 17 avril 2018 relative aux indices de référence.*

¹¹² *Loi du 16 juillet 2019 relative à l'opérationnalisation de règlements européens dans le domaine des services financiers.*

¹¹³ *Loi du 10 juillet 2020 instituant un Registre des fiducies et des trusts.*

¹¹⁴ *Loi du 30 mars 2022 relative aux comptes inactifs, aux coffres-forts inactifs et aux contrats d'assurance en déshérence.*

3.1.3.1. Requests for electronic information

Twelve of those texts enable to specifically request electronic information, meaning, data, although drafted all slightly differently, thus creating incoherences and confusion.¹¹⁵ Yet, three categories of requests can be inferred: those addressed to certain categories of OSPs, those addressed to any persons, and those addressed to specific entities.

The Law on the Financial Sector (Article 53.1.16), the Law on Market Abuse (Article 4.1.7), and the Law on Markets in Financial Instruments (Article 45.2.20) enable the CSSF to request data traffic records to providers of electronic communication services and public communication networks operators, meaning, OSPs, after judicial authorisation. The authorities would need, in these cases, ‘a reasonable suspicion of an infringement and [that] such records may be useful to ascertaining the truth in the context of an investigation’. In these cases, the CSSF will transfer a reasoned request to the Luxembourg district tribunal and an investigating judge will verify the justification and proportionality of the request.¹¹⁶ The order of the investigating judge is then subject to the same remedies (non-suspensive) as any order by the same judge.¹¹⁷ According to Article 133 of the Criminal Procedure Code,¹¹⁸ the public prosecutor and the suspect can lodge an appeal against the order of an investigative judge, as well as the plaintiff when it affects their civil interests. Here, the criminal provision does not seem adapted to the administrative proceedings, as they leave no room for an appeal by an investigated person who is not yet criminally charged. Furthermore, only a partial appeal by the CSSF is allowed.

No personal scope of application is specified in four texts,¹¹⁹ which could thus potentially include OSPs. This power can be used to request three

¹¹⁵ Law on the Financial Sector, article 53.1.4 and 16; Law on Institutions for Occupational Retirement Provision, Article 62.1.c; Law on Specialised Investment Funds, Article 45.3.d; Law on Payment Services, Article 58-5.1.4; Law on UCI, Article 147.2.d; Law on AIFM, Article 50.2.d; Law on Short Selling of Financial Instruments, Article 2, referring to Regulation (EU) 236/2012 of the European Parliament and of the Council of 14 March 2012 on Short Selling and certain aspects of Credit Default Swaps (regulation 236/2012), Article 33.2.d; Law on Market Abuse, Article 4.1.6 and 7; Law on Markets in Financial Instruments, Article 45.2.4 and 20; Law on Indices, Article 2.1.5; Law on Central Securities Depositories, Article 2.4; and, Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 7 referring to Law on AIFM, Article 50.2.d.

¹¹⁶ Article 53.3 of the Law on the Financial Sector, Article 5 of the Law on Market Abuse, and Article 45.3 of the Law on Markets in Financial Instruments.

¹¹⁷ Article 53.3 of the Law on the Financial Sector.

¹¹⁸ Articles 133, 134 and 134-1 detail the rules on the adversarial principle to the appeal.

¹¹⁹ Law on the Financial Sector, Article 53.1.4; Law on Specialised Investment Funds, Article 45.3.d; Law on AIFM, Article 50.2.d; Law on Short Selling of Financial Instruments, Article 2, referring to Regulation 236/2012, Article 33.2.d.

categories of existing data.¹²⁰ Firstly, all texts mention the request of recordings of telephone conversations. Secondly, most texts, except four of them,¹²¹ lists the request of electronic communications. Thirdly, texts usually mention other categories of data, in a non-harmonised manner: ‘other electronic exchanges’,¹²² ‘data’,¹²³ ‘traffic data’,¹²⁴ ‘records of data exchanges’,¹²⁵ and ‘electronic records’.¹²⁶

Under most legal frameworks, these requests can only be addressed to supervised or concerned entities according to the laws.¹²⁷ For instance, the Law on Market Abuse refers to data ‘held by the persons subject to [the] prudential supervision’ of the CSSF;¹²⁸ and the Law on Markets in Financial Instruments lists investment firms, credit institutions, ‘any other entity regulated by this Law or by Regulation (EU) No 600/2014’.¹²⁹ More precisely, the Law on Payment Services mentions ‘payment service providers authorised or registered in Luxembourg, the Luxembourg branches of payment service providers whose home Member State is a Member State other than Luxembourg and the agents established in Luxembourg to which these payment service providers have recourse, which provide transfer of funds services’.¹³⁰ However, these laws do not specify if data can only be requested to the investigated entity or also to another supervised entity as third-party. In that latter case, an OSP should qualify as a supervised entity to be the addressee of such a request.

3.1.3.2. Requests for information

More generally, all sectoral laws in the area of banking and financial markets grant the CSSF and the CAA ‘considerable powers to obtain the necessary information’.¹³¹ These powers are drafted as general bases to access

¹²⁰ It is therefore not possible to request the retention of future data.

¹²¹ Law on Specialised Investment Funds, Law on AIFM, Law on Short Selling of Financial Instruments, and the Law on Central Securities Depositories.

¹²² Law on the Financial Sector, Law on Institutions for Occupational Retirement Provision, Law on UCI, Law on Markets in Financial Instruments.

¹²³ Law on Specialised Investment Funds.

¹²⁴ Law on Payment Services, Law on Market Abuse, Law on Indices.

¹²⁵ Law on AIFM, Law on Short Selling of Financial Instruments.

¹²⁶ Law on Central Securities Depositories.

¹²⁷ Law on Institutions for Occupational Retirement Provision, Article 62.1.c; Law on UCI, Article 147.2.d; Law on Indices, Article 2.1.5; Law on Central Securities Depositories, Article 2.4.

¹²⁸ Article 4.1.6 of the Law on Market Abuse.

¹²⁹ Article 45.2.4 of the Law on Markets in Financial Instruments.

¹³⁰ Article 58-5.1.4 referring to Article 58-2 of the Law on Payment Services.

¹³¹ Limpach, Goergen, (n. 16), p. 181.

or request information.¹³² Regarding the access to documents, no personal scope is defined: such a request could be directed to OSPs. Regarding the request of information, there are three types of powers. Firstly, some laws grant a general power to request information to any person,¹³³ or restrictively any person with a link with the supervised activities,¹³⁴ or any professional.¹³⁵ This first category is broad enough to include OSPs. General powers to request any person within the framework of the law on markets in financial instruments is particularly supported by the ECJ case law.¹³⁶ According to the court, ‘competent authorities must have all supervisory and investigatory

¹³² Law on the Financial Sector, Article 53.1.1, 2 and 8 and Article 53.2.a; Insurance Sector Law, Article 4.b and e; Law on Investment Companies in Risk Capital, Article 32; Law on Institutions for Occupational Retirement Provision, Article 62.1.a and b; Law on Specialised Investment Funds, Article 45.3.a and b and Article 58; Law on Transparency Requirements, Article 22.2.a to c; Law on Payment Services, Article 31.4; Law on UCI, Article 147.2.a, b and h; Law on Mandatory Squeeze-Out and Sell-Out of Securities, Article 6-2.a and b; Law on AIFM, Article 50.2.a, b and h; Law on Short Selling of Financial Instruments, Article 2 referring to Regulation 236/2012, Article 33.2.a and b; Law on OTCD, Article 2.1.1 and 2; Law concerning the Audit Profession, Article 37; Law on Market Abuse, Article 4.1.1 to 3; Law on Payment Accounts, Article 31.1; Law implementing Regulation 2015/751, Article 2.1 and 2; Law on KID, Article 4.1.1 and 2; Law on Indices, Article 2.1.1 to 3; Law on Markets in Financial Instruments, Article 45.2.1, 2, 7 and 10; Law on Central Securities Depositories, Article 2.1 and 2; Law on Prospectuses for Securities, Article 7.2.1 to 3 and 12, Article 35.1 to 3, and Article 58.1; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 2.2.2 and 3, Article 7 referring to Article 50 of the Law on AIFM, Article 12.1 to 3, Article 17.2.1 and 2, Article 20-3.2.1 to 3, Article 20-9.2.1 to 3, and Article 20-16.2.1 to 3; Law establishing a IBAN Central Electronic Data Retrieval System, Article 4.1.a and b; Law establishing a Register of Fiducies and Trusts, Article 8.1.1, 2, 5 and 6; Law relating to the Issue of Covered Bonds, Article 20.1, 3 and 8; and, Law on Inactive Accounts, Article 40.1.1, 2 and 5.

¹³³ Law on the Financial Sector, Article 53.1.2; Insurance Sector Law, Article 4.e; Law on Specialised Investment Funds, Article 45.3.b; Law on UCI, Article 147.2.b; Law on Short Selling of Financial Instruments, Article 2 referring to Regulation 236/2012, Article 33.2.b; Law concerning the Audit Profession, Article 37; Law on Market Abuse, Article 4.1.2; Law implementing Regulation 2015/751, Article 2.2; Law on Markets in Financial Instruments, Article 45.2.2 and 10; Law on KID, Article 4.1.2; Law on Central Securities Depositories, Article 2.2; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 17.2.2; Law establishing a Register of Fiducies and Trusts, Article 8.1.2; Law on Inactive Accounts, Article 40.1.2.

¹³⁴ Activities of the manager of the alternative investment fund, Law on AIFM, Article 50.2.b; of a qualifying venture capital fund or social entrepreneurship fund or monetary fund, Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 2.2.3, Article 12.3, Article 20-3.2.3, and Article 20-9.2.3; of the issuance of covered bonds, Law relating to the Issue of Covered Bonds, Article 20.3.

¹³⁵ Law establishing a IBAN Central Electronic Data Retrieval System, Article 4.1.b; Law establishing a Register of Fiducies and Trusts, Article 8.6.

¹³⁶ Regarding Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments, replaced by Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014.

powers that are necessary for the exercise of their functions, including the rights to have access to any document and to demand information from any person'.¹³⁷ Secondly, some laws draft a specific power to request information to supervised entities¹³⁸ or generally entities related to the regulated activity.¹³⁹ In that case, an OSPs should qualify as such to have to answer a request for information. Thirdly, additionally, some laws specifically enable to request information from other entities.¹⁴⁰ For instance, the Law on Market Abuse extends these requests to any market participants,¹⁴¹ potentially, OSPs.

Under such a general power, the authorities can access any document, information, or data, under any format, and receive or realise their copy. Some texts specify that the accessed documents or data shall be likely to be relevant for the performance of authorities' supervisory mission,¹⁴² investigatory

¹³⁷ ECJ, *Annett Altmann and Others v. Bundesanstalt für Finanzdienstleistungsaufsicht*, 12.11.2014, C-140/13, § 29. Recalled in ECJ, *Bundesanstalt für Finanzdienstleistungsaufsicht v. Ewald Baumeister*, 19.06.2018, C-15/16, ¶ 29; ECJ, (n. 16), § 34.

¹³⁸ Law on the Financial Sector, Article 53.2.a; Insurance Sector Law, Article 4.b; Law on Investment Companies in Risk Capital, Article 32; Law on Institutions for Occupational Retirement Provision, Article 62.1.b; Law on Specialised investment funds, Article 58; law on payment services, Article 31.4; law on payment accounts, Article 31.1; law on the Operationalisation of European Regulations in the Area of Financial Services, Article 2.2.2, Article 12.2, Article 20-3.2.2, and Article 20-9.2.2. Supervised entities can be extended to related entities. Extension to entities who 'act in concert with them and persons who control them or are controlled by them', Law on Mandatory Squeeze-Out and Sell-Out of Securities, Article 6-2.a; extension to 'non-financial counterparties, central counterparties and trading venues', Law on OTCD, Article 2.1.2. The literature considers that these should extend to other, non-supervised entities, particularly to assess if they should be supervised, Limpach, Goergen, (n. 15), p. 182.

¹³⁹ Entities linked to the definition and provision of indices, Law on Indices, Article 2.1.2; Law on Prospectuses for Securities, Article 7.2.1 and 2 and 12, Article 35.1 and 2, and Article 58.1, particularly issuers, offerors or guarantors; entities and persons linked to crowdfunding service providers for business, Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 20-16.2.1; trustees and fiduciaries of the investigated fiducie or trust, Law establishing a Register of Fiducies and Trusts, Article 8.5.

¹⁴⁰ Such as approved statutory auditors, Law on the Financial Sector, Article 53.1.8; Law on Payment Services, Article 31.4 and Article 58-5.8; Law on Mandatory Squeeze-Out and Sell-Out of Securities, Article 6-2.b; Law on Markets in Financial Instruments, Article 45.2.7; Law on Prospectuses for Securities, Article 7.2.3, and Article 35.3; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 20-16.2.1 and 3; Law relating to the Issue of Covered Bonds, Article 20.8; Law on Inactive Accounts, Article 40.1.5. Entities linked to securities admitted to trading on a regulated market, Law on Transparency Requirements, Article 22.2.a to c. Or operators under Law on Indices, Article 2.1.3.

¹⁴¹ Law on Market Abuse, Article 4.1.3.

¹⁴² Law on the Financial Sector, Article 53.1.1; Insurance Sector Law, Article 4.b; Law on Markets in Financial Instruments, Article 45.2.1.

mission,¹⁴³ functions,¹⁴⁴ or duties.¹⁴⁵ Considering that the authorities can impose sanctions under all those frameworks, the term of ‘supervision’ does not seem adapted, as these powers are actually aimed at administrative investigatory proceedings. Therefore, it appears that the use of the powers to request information is not limited to already opened investigations but can also be used outside of them. Other texts specify that the requested documents or data shall be relevant,¹⁴⁶ particularly ‘for the exercise of its tasks’¹⁴⁷ or missions.¹⁴⁸ Additionally, the Insurance Sector Law highlights that the CAA should implement its powers ‘promptly and in a proportionate manner’.¹⁴⁹

Only Article 31.4 of the Law on Payment Services details the content of the request, which should specify its purpose and a deadline. Only the Law on the Operationalisation of European Regulations in the Area of Financial Services specifies that the requested information shall be provided without delay.¹⁵⁰ According to Article 53.2.a of the Law on the Financial Sector, the CSSF can also request supervised entities to provide information on a regular basis and in a specified format. It should be mentioned that the CSSF is developing secured application programming interfaces to enable the interconnections of systems for automatised transfer of data.¹⁵¹ Both Article 4.1.3 of the Law on Market Abuse and Article 2.1.3 of the Law on Indices enable to request information to market participants and operators through standardised formats, reports on transactions or through a direct access to their systems.

3.1.3.3. Common rules

Under both types of powers (general or specific), the addressee usually cannot refuse the answer the request of the authority due to the professional

¹⁴³ Law relating to the Issue of Covered Bonds, Article 20.1.

¹⁴⁴ Law on Inactive Accounts, Article 40.2.1.

¹⁴⁵ Law on Specialised Investment Funds, Article 58.

¹⁴⁶ Law on Markets in Financial Instruments, Article 45.2.2; or necessary, Insurance Sector Law, Article 4.e.

¹⁴⁷ Law on Payment Services, Article 31.4.

¹⁴⁸ Law on the Financial Sector, Article 53.2.a, regarding requests to supervised entities; Law on Investment Companies in Risk Capital, Article 32; Law on Payment Accounts, Article 31.1.

¹⁴⁹ Insurance Sector Law, Article 4.k.

¹⁵⁰ Law on the Operationalisation of European Regulations in the Area of Financial Services, Articles 2.2.2, 12.2, 20-3.2.2 and 20-9-2.2.

¹⁵¹ CSSF, *Rapport annuel 2022 Retour sur les activités et initiatives de la CSSF en 2022*, Luxembourg, 2023, p. 13.

secrecy.¹⁵² On the contrary, the powers of the CSSF under the law on market abuse apply ‘without prejudice to the legal provisions on professional secrecy’.¹⁵³

To enforce these powers, the CSSF can adopt coercive fines to compel addressees to cooperate under the Law on the Financial Sector. These fines can amount to a maximum of 1.250 euros per day, and a maximum total amount of 25.000 euros against supervised entities, ‘on the grounds of an observed failure to perform’.¹⁵⁴ The CAA can impose coercive fines of the same amount on supervised entities in order to compel them to answer a request.¹⁵⁵

Differently, other laws enable to sanction addressees who failed to cooperate. The sanctions can be directed against any addressee in certain laws;¹⁵⁶ while, in others, only supervised¹⁵⁷ or concerned¹⁵⁸ entities or ‘entities obliged to provided information’ can be sanctioned.¹⁵⁹ It should be mentioned that the sanction of supervised entities for not providing

¹⁵² Law on the Financial Sector, Article 41.1 and 2; Insurance Sector Law, Article 300.2.a; Law on Payment Services, Article 30.1; Law on Markets in Financial Instruments, Article 43.2; Law concerning the Audit Profession, Article 28.3, recalled in Law on Investment Companies in Risk Capital, Article 27.3.

¹⁵³ Law on Market Abuse, Article 4.2.

¹⁵⁴ Law on the Financial Sector, Article 63.3. Although coercive fines are provided for the enforcement of other powers of the CSSF, they are not applicable in case of refusal to comply with a request for information, under Article 58-5.2 of the Law on Payment Services, Article 3.3 of the Law implementing Regulation 2015/751 and Article 4.3 of the Law establishing a IBAN Central Electronic Data Retrieval System.

¹⁵⁵ Insurance Sector Law, Article 305.

¹⁵⁶ Law on Market Abuse, Article 12.4; Law on Markets in Financial Instruments, Article 47.4; Law on KID, Article 5.3; Law on Indices, Article 4.1; Law on Central Securities Depositories, Article 5.3; Law on Prospectuses for Securities, Article 12.3; Law on Inactive Accounts, Article 41.2; Law on the operationalisation of European regulations in the area of financial services, Article 3.2, Article 8.2, Article 13.2, Article 18.2, Article 20-4.1, Article 20-10.1, Article 20-17.3; Law establishing a IBAN Central Electronic Data Retrieval System, Article 5.3; Law establishing a Register of Fiducies and Trusts, Article 9.4.

¹⁵⁷ Law on the Financial Sector, Article 63.1; Insurance Sector Law, Article 303.1 and 2a; law on institutions for Occupational Retirement Provision, Article 65.1; Law on UCI, Article 148.1; Law on AIFM, Article 51.1; Law on OTCD, Article 3.1; approved statutory auditors, approved audit firms and audit firms only, Law concerning the Audit Profession, Article 43.1; Law on Payment Accounts, Article 32.1; Law implementing Regulation 2015/751, Article 3.1; Law relating to the Issue of Covered Bonds, Article 23.

¹⁵⁸ Such as the directors, managers, and liquidators of supervised entities, Law on Payment Services, Article 46.1; Law relating to the Issue of Covered Bonds, Article 23; Law on Investment Companies in Risk Capital, Article 17.1; Law on Institutions for Occupational Retirement Provision, Article 65.1; Law on Specialised Investment Funds, Article 51.1; Law on UCI, Article 148.1.

¹⁵⁹ Law on Transparency Requirements, Article 25.1; Law on Short Selling of Financial Instruments, Article 7.1.

information that could incriminate them has been criticised by the literature¹⁶⁰ as well as by the State Council (*Conseil d'Etat*).¹⁶¹ Thus, even when OSPs can be requested to provide information, they might not be sanctionable.

These provisions usually sanction (1) the refusal to provide the information,¹⁶² and/or (2) the provision of incomplete, incorrect, or false¹⁶³ information. Some laws only sanction this second category when committed knowingly¹⁶⁴ or purposefully.¹⁶⁵ The sanctions usually include an administrative fine. Most fines amount to between 250 and 250.000 euros.¹⁶⁶ Some laws provide for lesser fines,¹⁶⁷ while other set fines up to 5.000.000

¹⁶⁰ Lutgen, Marty, (n. 18), p. 52.

¹⁶¹ Conseil d'Etat, Avis complémentaire sur le projet de loi portant modification de la loi du 9 mai 2006 relative aux abus de marché et portant complément de transposition de la directive 2003/6/CE du Parlement européen et du Conseil du 28 janvier 2003 sur les opérations d'initiés et les manipulations de marché (abus de marché), 06/07/2010, 48.602, p. 2.

¹⁶² Except Law on the Operationalisation of European Regulations in the Area of Financial Services, Articles 3.2, 13.2, 18.2, 20-4.1, 20-10.1, and 20-17.3; Law establishing a IBAN Central Electronic Data Retrieval System Article 5.3; Law establishing a Register of Fiducies and Trusts, Article 9.4; Law relating to the Issue of Covered Bonds, Article 23. However, a refusal to answer a request could be penalised as an obstruction to the missions of the CSSF.

¹⁶³ However, some laws do not sanction when the information provided is false: Law on Transparency Requirements, Article 25.1; Law on Central Securities Depositories, Article 5.3; Law on Prospectuses for Securities, Article 12.3; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 3.2, Article 8.2 Article 13.2, Article 18.2, Article 20-4.1, Article 20-17.3; Law on Inactive Accounts, Article 41.2.

¹⁶⁴ Law on Markets in Financial Instruments, Article 47.4; Law on KID, Article 5.3; Law on Indices, Article 4.1; Law on Central Securities Depositories, Article 5.3; Law on Prospectuses for Securities, Article 12.3; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 3.2, Article 8.2, Article 13.2, Article 18.2, Article 20-10.1, Article 20-17.3; Law on Inactive Accounts, Article 41.2; Law establishing a Register of Fiducies and Trusts, Article 9.4; Law relating to the Issue of Covered Bonds, Article 23.

¹⁶⁵ Law establishing a IBAN Central Electronic Data Retrieval System, Article 5.3.

¹⁶⁶ Law on the Financial Sector, Article 63.2; against insurance and reinsurance undertakings under the Insurance Sector Law, Article 303.1; Law on Institutions for Occupational Retirement Provision, Article 65.2; Law on Transparency Requirements, Article 25.1; Law on AIFM, Article 51.2; Law on Market Abuse, Article 12.4; Law on Payment Accounts, Article 32.2, although here the minimum fine is of 251 euros; Law implementing Regulation 2015/751, Article 3.2; Law on KID, Article 5.3; law on Central Securities Depositories, Article 5.3; Law on Prospectuses for Securities, Article 12.3; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 3.2, Article 8.2, Article 13.2, Article 18.2, Article 20-10.2, Article 20-17.3; Law on Inactive Accounts, Article 41.2; Law establishing a IBAN Central Electronic Data Retrieval System, Article 5.3; Law establishing a Register of Fiducies and Trusts, Article 9.4.

¹⁶⁷ Such as a fine of between 15 to 500 euros under Article 17.1 of the Law on Investment Companies in Risk Capital; between 125 to 12.500 euros under Article 51.1 of the Law on Specialised Investment Funds, Article 46.1 of the Law on Payment Services, and Article 7.1 of the Law on Short Selling of Financial Instruments; up to 50.000 euros against supervised entities other than insurance and reinsurance undertakings under the Insurance Sector Law,

euros, or, alternatively, a fine up to 10% of the total annual turnover, or twice the amount of the benefit (if known) derived from the infringement.¹⁶⁸ Some other types of sanctions are also included, such as a warning or a reprimand,¹⁶⁹ or a public statement or an order to cease the infringement.¹⁷⁰

Criminal sanctions can also be imposed against addressees who failed to cooperate. Firstly, under Article 26 of the Law on Transparency Requirements, any person ‘who knowingly disclose to the CSSF [...] inaccurate or incomplete information shall incur a fine of between 250 and 125.000 euros’. Secondly, obliged entities under Article 7.3 of the Law on Mandatory Squeeze-Out and Sell-Out of Securities can be sanctioned by ‘imprisonment of between eight days and five years and a fine of between 251 and 125.000 euros or only one of these sanctions’ when giving knowingly ‘false or incomplete information in relation with their shareholdings or with a mandatory squeeze- or sell-out transaction’.

Various rules can protect the interests of the persons concerned by the requests for information sent by the CSSF or the CAA. Several laws provide that, unless there is a risk that the situation may deteriorate, the decisions are taken after an adversarial investigation.¹⁷¹ Also, various laws provide for the communication of the decision to the concerned supervised entity or person.¹⁷² Regarding the motivation of the decisions, it is explicit in some

Article 303.1. Differently, Article 3.3 of the Law on OTCD sets up a fine between 125 and 1.500.000 euros.

¹⁶⁸ Law on the Financial Sector, Article 63-2a.4; Law on UCI, Article 148.4; Law on Markets in Financial Instruments, Article 47.4; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 20-4.2; Law relating to the Issue of Covered Bonds, Article 23. Article 4.2 of the Law on Indices does not set a fixed fine but only a maximum fine up to three times the amount of the profits gained or losses avoided because of the infringement where those can be determined.

¹⁶⁹ Law on the Financial Sector, Article 63.2; Insurance Sector Law, Article 303.2; Law on Institutions for Occupational Retirement Provision, Article 65.1; Law on AIFM, Article 51.2; Law on OTCD, Article 3.3; Law on Payment Accounts, Article 32.2; Law implementing Regulation 2015/751, Article 3.2.

¹⁷⁰ Law on the Financial Sector, Article 63-2a.4; Law on UCI, Article 148.4; Law concerning the Audit Profession, Article 43.3; Law on Markets in Financial Instruments, Article 47.6; Law on Indices, Article 4.2; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 20-4.2, and, only mentioning the public statement, Article 20-10.2; Law relating to the Issue of Covered Bonds, Article 23.

¹⁷¹ Insurance Sector Law, Article 303.4, including the right to be assisted or represented; Law on Institutions for Occupational Retirement Provision, Article 66.1; Law on Investment Companies in Risk Capital, Article 16.1; Law on Institutions for Occupational Retirement Provision, Article 66.1; Law on Specialised Investment Funds, Article 45.1; Law on UCI, Article 142.1; Law on AIFM, Article 52.1; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 52.

¹⁷² Insurance Sector Law, Article 307; Law on Investment Companies in Risk Capital, Article 16.1; Law on Institutions for Occupational Retirement Provision, Article 66.1; Law on

laws.¹⁷³ However, Articles 24 and 24-18 of the law on payment services only provides for the motivation of decisions which includes ‘penalties or restrictions on the freedom to establish branches, to use agents or to provide services’. Once the addressee has provided information at the request of the authorities, the interest of the concerned person is protected by the professional secrecy applicable to the CSSF and the CAA, criminalising the disclosure of confidential information.¹⁷⁴ However, it remains unclear if a request for information is considered as an administrative decision or a mere investigatory step. In any case, these rules will be applicable to a decision on sanctioning an OSP.

Some definitive decisions, especially on imposing sanctions, must be published, while it is a mere possibility for others. However, when the publication is disproportionate, on the basis of a case-by-case assessment, the decision may not be disclosed or only disclosed partially or anonymously.¹⁷⁵

Payment Services, Articles 24 and 24-18; Law on Specialised Investment Funds, Article 45.1; Law on AIFM, Article 52.1.

¹⁷³ Law on the Financial Sector, Article 53.4 regarding supervisory powers, and Article 63-4 regarding administrative sanctions; Insurance Sector Law, Article 307; Law on Investment Companies in Risk Capital, Article 16.1; Law on Institutions for Occupational Retirement Provision, Article 66.1; Law on Specialised Investment Funds, Article 45.1; Law on UCI, Article 142.1; Law on AIFM, Article 52.1; Law on Prospectuses for Securities, Articles 15, 35 and 61; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 52; Law relating to the Issue of Covered Bonds, Article 23.3.

¹⁷⁴ Article 16 of the Law creating the CSSF, recalled in Law on the Financial Sector, Article 44; Insurance Sector Law, Article 7; Law on Investment Companies in Risk Capital, Article 15; Law on Institutions for Occupational Retirement Provision, Article 59; Law on Payment Services, Article 32; Law on UCI, Article 134; Law on AIFM, Article 47.3; Law on Payment Accounts, Article 3.2; Law on Markets in Financial Instruments, Article 50; Law on Short Selling of Financial Instruments referring to Regulation 236/2012, Article 34. According to the ECJ, confidential information must not be public and its disclosure ‘is like y to affect adversely the interests of the natural or legal person who provided that information or of third parties, or the proper functioning of the [prudential] system’, ECJ, (n. 137), ¶ 46. See C. Farinhas, ‘Access to confidential information in the financial and banking sectors: judgements of the Court of Justice in Altmann, Baumeister, UBS and Buccioni’, *Law and Financial Markets Review*, Routledge, 02/10/2019, vol. 13, no. 4, pp. 203-210, DOI:10.1080/17521440.2019.1668130.

¹⁷⁵ Law on the Financial Sector, Article 63.2; Insurance Sector Law, Article 306; Law on Institutions for Occupational Retirement Provision, Article 67-1; Law on Prospectuses for Securities, Article 14; Law on Transparency Requirement, Article 26b; Law on Payment Services, Article 46.3; Law on Short Selling of Financial Instruments, Article 7.2; Law on AIFM, Article 51.2; Law on Specialised Investment Funds, Article 51.3; Law on Payment Accounts, Article 32.3; Law on Markets in Financial Instruments, Article 49.1; Law on Central Securities Depositories, Article 7.1; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 5.1, Article 10.1, Article 15.1, and Article 20-12.1; Law establishing a IBAN Central Electronic Data Retrieval System, Article 5.6; Law establishing a Register of Fiducies and Trusts, Article 9.9; Law relating to the Issue of Covered Bonds, Article 25.2; Law on Inactive Accounts, Article 44.1.

Such a publication supposes that the consequences of the publication might be worse than the impact on the reputation of the concerned person, and are independent from the seriousness of the infringement.¹⁷⁶ Yet, the exception to publication is not contemplated in some laws.¹⁷⁷ Various laws specify that no publication is required for ‘decisions imposing measures that are of an investigatory nature’.¹⁷⁸

Regarding remedies, for the investigated person or the sanctioned addressee of a request for information, most laws provide that decisions concerning fines can be ‘referred to the administrative tribunal which deals with the substance of the case’ within one month¹⁷⁹ from the notification of the decision.¹⁸⁰ Other laws provide for a full review of the merits of the decision by the administrative tribunal,¹⁸¹ within one month from the date of notification of the decision.¹⁸² For the laws which do not set a delay for this remedy,¹⁸³ Article 13.1 of the Law on the Rules of Procedure before the Administrative Tribunals¹⁸⁴ sets a three-month delay from the moment of the

¹⁷⁶ Cour administrative, 19.07.2023, no. 48647C; based on Tribunal of the EU, *VQ v. European Central Bank*, 08.07.2020, T-203/18.

¹⁷⁷ Law on UCI, Article 149; Law on OTCD, Article 3.4; Law on Market Abuse, Article 14; Law on KID, Article 7; Law on Indices, Article 4.5; Law on the Operationalisation of European Regulations in the Area of Financial Services, Article 20-6.

¹⁷⁸ Law on the Financial Sector, Article 63-3a; Law on Institutions for Occupational Retirement Provision, Article 67-1; Law on UCI, Article 149.1; Law on Markets in Financial Instruments, Article 49.1, Law on the Operationalisation of European Regulations in the Area of Financial Services, Articles 5.1, 10.1, 15.1, and 20-12.1.

¹⁷⁹ Law on the Financial Sector, Article 63.2 and Article 63-5; Law on Investment Companies in Risk Capital, Article 16.2; Law on Specialised Investment Funds, Article 45.2; Law on AIFM, Article 52.2; Law on Payment Services, Article 46.4; Law on Payment Accounts, Article 33; Law implementing Regulation 2015/751, Article 3.4; Law on Markets in Financial Instruments, Article 65; Law on KID, Article 6; Law on Indices, Article 4.4; Law on Central Securities Depositories, Article 8; Law on the Operationalisation of European Regulations in the Area of Financial Services, Articles 4, 9, 14, 19, 20-5, 20-11 and 20-20. Article 8 of the Law on Short Selling of Financial Instruments provides for the same remedy, although in a three-month delay.

¹⁸⁰ However, various laws do not include this comment on the start of the delay: Law on the Financial Sector, Article 63.2 and Article 63-5; Law on Payment Services, Article 46.4; Law on KID, Article 6; Law on Indices, Article 4.4; Law on the Operationalisation of European Regulations in the Area of Financial Services, Articles 4, 9, 14, 19, 20-5, 20-11 and 20-20.

¹⁸¹ Articles 15, 35 and 61 of the Law on Prospectuses for Securities and Article 4 of the Law on OTCD provide that the decisions of the CSSF can ‘be subject to a right to apply for reversal with the administrative tribunal’.

¹⁸² Insurance Sector Law, Article 307; Law establishing a IBAN Central Electronic Data Retrieval System, Article 6; Law establishing a Register of Fiducies and Trusts, Article 10; Law relating to the Issue of Covered Bonds, Article 24.

¹⁸³ Law on Transparency Requirement, Article 27; Law concerning the Audit Profession, Articles 46 and 43.5; Law on Market Abuse, Article 15.

¹⁸⁴ *Loi du 21 juin 1999 portant règlement de procédure devant les juridictions administratives.*

notification of the decision or the date the person acquired knowledge of it. More problematically, no specific information on the remedies is to be found in the Law on Specialised Investment Funds, and the Law on Inactive Accounts. In that case, an action for annulment is generally open in front of the administrative tribunal.

3.1.4. Competition law enforcement

On the one hand, Article 24 of the Competition Law enables the Competition Authority to collect, upon invitation, any information, document, or justification, ‘in whatever hands they may find themselves’,¹⁸⁵ for instance in the ones of the OSPs. The authority can also request access to software and retained data when the investigation relates to ‘operations involving the use of information technology’.¹⁸⁶ In that case, the data should be provided ‘in clear’, meaning, for instance, not encrypted; and the authority can request the transcription of the documents. In both cases, the information must support the authority’s mission or be necessary to the control. According to Article 8 of the law on mergers bill,¹⁸⁷ these powers will be extended also to merger control carried out by the Competition Authority.

On the other hand, Article 27 of the Competition Law provides for a general power to request information necessary to carry out the missions of the authority or likely to be relevant.¹⁸⁸ Such a request can be addressed to undertakings and associations of undertaking, meaning ‘any entity carrying on an economic activity, regardless of its legal status or method of financing’,¹⁸⁹ as well as to any legal or natural person.¹⁹⁰ Such a broad definition would thus include OSPs, most of them being undertakings and legal persons. In particular, the request is not limited to information retained but can be extended to any information the addressee has access to.¹⁹¹

Under both provisions, investigative powers require the previous opening of a procedure by the Competition Authority itself or following a complaint.¹⁹² The investigation is directed by a head investigator.¹⁹³ The

¹⁸⁵ Article 24.4 of the Competition Law.

¹⁸⁶ Article 24.5 of the Competition Law.

¹⁸⁷ *Projet de loi 8296 relative au contrôle des concentrations entre entreprises et portant modification de: 1° la loi modifiée du 10 août 1915 concernant les sociétés commerciales ; 2° la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; 3° la loi modifiée du 7 décembre 2015 sur le secteur des assurances ; 4° la loi modifiée du 30 novembre 2022 relative à la concurrence.*

¹⁸⁸ Article 27.1 and 2 of the Competition Law.

¹⁸⁹ Article 27.1 of the Competition Law in relation to Article 2.7.

¹⁹⁰ Article 27.2 of the Competition Law.

¹⁹¹ Article 27.1 of the Competition Law.

¹⁹² Article 21 of the Competition Law.

¹⁹³ Article 23 of the Competition Law.

decision to request information shall include, under penalty of nullity, the object and aim of the control,¹⁹⁴ and the legal basis and aim of the request.¹⁹⁵ In that latter case, the request should be proportionate and not lead the addressee, when it is an undertaking, to admit the existence of an infringement to competition law.¹⁹⁶ Also, the Competition Authority shall set a reasonable delay to answer a request of information directed to undertakings, and a specific and reasonable delay to answer a request directed to any other person.¹⁹⁷

Coercive fines can be adopted against undertakings, including OSPs, only when failing to provide accurate, complete, and non-misleading information within the deadline.¹⁹⁸ The decision is adopted by the College of the authority after notification to the undertaking of its right to be heard. The sanction can amount up to 5% of the global medium daily turnover of the preceding business year for each day of delay.¹⁹⁹ If the undertaking does not answer within the delay or provides an inaccurate, incomplete or misleading information, intentionally or negligently, the College can adopt a fine, after notification to the undertaking of its right to be heard. The fine can amount up to 1% of the global turnover of the preceding business year.²⁰⁰ No sanctions are provided regarding powers to request information based on Article 24.

Various safeguards are dedicated to protecting the interests of the investigated undertaking. Firstly, the agents of the authority shall respect the professional secrecy of their function.²⁰¹ Thus, the information gathered shall only be used for limited purposes, meaning these linked to the missions of the authority. Secondly, a number of procedural guarantees are introduced in order to guarantee the adversarial principle. The undertakings are notified of the objections raised against them, and they can submit observations within a period of at least a month.²⁰² Once notified, they have access to the file of the investigation, with exception to, for instance, confidential data and information protected by the secrecy of communications between lawyers and their clients.²⁰³ Thirdly, at any moment of the investigation, interested persons can request a confidential processing of the information provided or

¹⁹⁴ Article 24 of the Competition Law.

¹⁹⁵ Article 27 of the Competition Law.

¹⁹⁶ Article 27.1 of the Competition Law.

¹⁹⁷ Article 27 of the Competition Law.

¹⁹⁸ Article 27 of the Competition Law.

¹⁹⁹ Article 31 of the Competition Law.

²⁰⁰ Article 32 of the Competition Law.

²⁰¹ Both public servants and investigators take an oath on that regard, Articles 9, 18.2 and 19.2 of the Competition Law.

²⁰² Article 37.1 of the Competition Law.

²⁰³ Articles 38 and 39 of the Competition Law.

accessed.²⁰⁴ The decision of the head investigator in that respect is notified and can be appealed in front of the President of the Competition Authority. The maintaining of confidentiality of the information is then decided upon by the appointed magistrate, who shall not be a member of the College which will decide on the case.²⁰⁵ Finally, once a decision has been adopted by the Competition Authority, the concerned person has the right to lodge a complaint in front of the administrative tribunal.²⁰⁶

Various safeguards are provided for third parties, such as OSPs, requested by the Competition Authority to transfer information. Firstly, a control under Article 24 of the competition law must be notified to the head of the undertaking or the occupier of the premises or their representative. Following the control, a record is drafted by the agents and signed by the head of the undertaking or the occupier of the premises or their representative, who receives a copy of the document. Secondly, the addressee can benefit from the same safeguards as the concerned person (see *supra*) when a decision of penalties or fine has been adopted against them. This concerns in particular the right to be heard, the right to request the confidential processing of information or the right to a remedy. However, the right to appeal in front of an administrative tribunal directly against a decision to request information has been denied, since it does not qualify an administrative decision. The legality and the merits of such a request can only be challenged if a sanctioning decision is adopted. The administrative tribunal considered that offering a right to complaint against these requests would multiply the appeals and prolong the investigation, while the objectives of these sanctions are primarily dissuasive. According to the judges, in such context, the denial of remedy is necessary for the efficiency of competition law.²⁰⁷

3.1.5. GDPR enforcement

The CNPD can ‘access all personal data and to all information necessary for the performance of its tasks’.²⁰⁸ However, this power seems limited to request information from the data controller and the data processor affected by the investigation. However, the law does not provide an explicit

²⁰⁴ Article 33 of the Competition Law. The request must be written and specially motivated.

²⁰⁵ Article 34 of the Competition Law. The interested person can request to be heard by the magistrate. The final decision by the magistrate cannot be appealed in front of courts.

²⁰⁶ Article 63 of the Competition Law. However, against a decision on penalties and fines, any element that could have led to a complaint during the investigation cannot be questioned in front of the judge.

²⁰⁷ Tribunal administratif, (n. 34). On the contrary, for a direct remedy against a request for information by the European Commission, see Tribunal of the EU, *Cemex SAB de CV and Others v. European Commission*, 14.03.2014, T-292/11.

²⁰⁸ Article 58.1.e of the GDPR and Article 14.1 of Law organising the CNPD.

power to request information from third parties such as OSPs if they are not under investigation.

The Internal Rules on the Investigative Procedure²⁰⁹ grant the power to request information to third parties, however without imposing an obligation on that third party to respond to the request. Yet, the normative instrument used to extend investigatory powers can be debated, as these must usually be modified by laws, and not based on internal rules. Nevertheless, such an extension is in conformity with the interpretation of the GDPR by the ECJ: authorities should ‘possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties’.²¹⁰ As underlined by European institutions, ‘the powers of the supervisory authority must be interpreted broadly to ensure full effectiveness of data protection for data subjects in the EU’.²¹¹ Since that power is granted under Internal Rules, it should not be possible to enforce them through the GDPR²¹² or national sanctions.²¹³

Whenever an investigation is open,²¹⁴ the Internal Rules provide that the head investigator can request any document on any support, including to make a copy of it, and access any electronic program or data and their transcription.²¹⁵ According to these rules, the professional secrecy cannot justify a refusal to answer a request.²¹⁶ The request must focus on useful data, documents necessary for the performance of the investigation, or any information and justification useful and necessary for the completion of the

²⁰⁹ *Règlement relatif à la procédure d'enquête*, from 22.01.2020.

²¹⁰ ECJ, *Maximilian Schrems v. Data Protection Commissioner (Schrems I)*, 06.10.2015, C-362/14, ¶ 43.

²¹¹ European Union Agency for Fundamental Rights et al., *Handbook on European data protection law*, Luxembourg, Publications Office of the EU, 2018, p. 195, DOI:10.2811/58814.

²¹² Article 83.5.e of the GDPR, referred to by Article 48 of the Law organising the CNPD: ‘administrative fines up to 20.000.000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher’.

²¹³ Article 49 of the Law organising the CNPD: coercive fine of up to 5 per cent of the average daily turnover for the previous financial year, or for the last financial year for which the accounts have been closed, for each day of delay from the date set by the Board in its decision.

²¹⁴ However, the opening of an investigation by the CNPD requires a very low threshold of clues of non-compliance to the GDPR, V. Wellens, ‘RGPD – Procédures préalables à une décision de l’autorité nationale de contrôle et devant les tribunaux’, *Articles LexNow*, 03.06.2019. It can be proposed by any member of the college to the whole college, at any time, by written or oral means, and this proposition must be approved at the majority by the college, Article 38 of the Law organising the CNPD and Article 2 of the Internal Rules on the Investigation Procedure.

²¹⁵ Article 8.2 of the Internal Rules on the Investigation Procedure.

²¹⁶ Article 8.2 of the Internal Rules on the Investigation Procedure, in application of Article 67 of the Law organising the CNPD, considering the professional secrecy of lawyers, notaries and audit professionals.

investigation.²¹⁷ If applicable, the rules require the requested person to transcribe electronic program or data into documents that can be used directly for the investigation.²¹⁸ Despite the lack of official interpretation of this provision, it might be construed as allowing to request intelligible data, meaning that it should not be encrypted, or containing an explanation of the relevant algorithms.²¹⁹

The data controller or processor under investigation benefit from various safeguards during the investigation. The decision to open an investigation, can be appealed in front of the administrative tribunal.²²⁰ The investigation must be both incriminating and exculpatory and must respect the adversarial principle.²²¹ Once evidence of violations of the GDPR are found, they must be notified to the concerned controller or processor, which can then provide written observations in the delay set by the head investigator (at least 15 days). If the head investigator responds to the inspected person's observations, the latter has a second opportunity to provide observations (within 15 days).²²² The investigated person (and their lawyer if designated) can request access to the case file.²²³ The collegial formation adopting the final decision shall be independent, meaning, the head investigator will not be part of it.²²⁴ The final decision of the CNPD can be appealed in front of the administrative tribunal.²²⁵

Considering that the safeguards are designed for the investigated person and that the request for data does not qualify as an administrative decision, the third parties receiving such a request have no specific remedies.

3.2. Administrative requests to online service providers: the bigger picture

Despite the apparent broadness of the powers of competent authorities to request information, including data, to third parties, such as OSPs, this power is particularly intrusive to fundamental rights, mainly, the right to privacy. Such an assessment has already been highlighted by the ECtHR in

²¹⁷ Article 8.2 of the Internal Rules on the Investigation Procedure.

²¹⁸ Article 8.2 of the Internal Rules on the Investigation Procedure.

²¹⁹ By comparison, rights to access and to portability, Articles 15 and 20 of the GDPR.

²²⁰ Article 55 of the Law organising the CNPD.

²²¹ Articles 39 and 40 of the Law organising the CNPD.

²²² Article 8.3 of the Internal Rules on the Investigation Procedure.

²²³ Article 8.4 of the Internal Rules on the Investigation Procedure.

²²⁴ Article 41 of the Law organising the CNPD. To avoid any other interest conflict, investigators can also be replaced, Article 5 of the Internal Rules on the Investigation Procedure.

²²⁵ Article 55 of the Law organising the CNPD.

the context of criminal proceedings.²²⁶ According to the European Production Order Regulation, in criminal proceedings, the request for content data and most traffic data must be authorised by a judge. The ECJ highlighted, as in that regulation, that other types of data, particularly data requested for the sole purpose of identifying the user, interfere in a lesser extent with the right to privacy, and can thus be requested by an administrative authority with no need for a prior judicial control.²²⁷ However, in Luxembourg, it does not seem to be authorised for administrative authorities to require in a compelling way any type of data to OSPs. In order to reflect whether such a power could be granted to those authorities it is then necessary to examine these investigatory powers within the constitutional framework, as well as in light of the Law on the Electronic Communications Sector.

Article 28 of the former Constitution of 1868 safeguarded the secrecy of letters and telegrams, primarily understood as protecting the privacy of their contents. In contrast, Article 30 of the new Constitution of 2023 broadly ensures the inviolability of communications, a right that may be limited by law.²²⁸ This updated approach to communications aims to align the constitutional text with the rapid advancements of technology. The concept of ‘communications’ is understood by the literature as including ‘correspondence, which is written, whatever its form (letters, facsimiles, e-mails, SMS (Short Message Service), MMS (Multimedia Messaging Service); dialogue (live, by telephone); and audiovisual communication (FaceTime, etc.)’.²²⁹ The term receives a definition under the Law on the Electronic Communications Sector: ‘any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service’.²³⁰ If the information is not directed towards a specific group, such as a publication visible to anyone with an account on a website or within a group (e.g. on Facebook) that is not accessible to a general visitor, it is possible that the criterion of a ‘determined number of parties’ is not fulfilled. In such cases, the published information may not be regarded as a communication, and hence, would not be protected under the right of the inviolability of communications. Moreover, this definition does not clarify whether traffic data associated with these communications falls within the scope of the term ‘communication’. The literature suggests that the inviolability of communications pertains solely to the content of the

²²⁶ ECtHR, *Benedik v. Slovenia*, 24.04.2018, no. 62357/14; ECtHR, *Ringler v. Austria*, 12.05.2020, no. 2309/10.

²²⁷ ECJ, *La Quadrature du Net and Others v. Premier ministre and Ministère de la Culture*, 30.04.2024, C-470/21.

²²⁸ The right to privacy is more generally protected at Article 11.3 of the Constitution.

²²⁹ A. Steichen, *La constitution luxembourgeoise commentée*, Bertrange, Legitech, 2024, p. 167.

²³⁰ Article 2.d of the Law on the Electronic Communications Sector.

message.²³¹ By opposition, another author extends the notion of communication to traffic data.²³² In sum, from a constitutional perspective, the protection of traffic data remains unclear.

The Law on the Electronic Communications Sector regulates the access to retained data by providers of electronic communication services and public communication networks operators. As a principle, electronic communications are confidential, including traffic data.²³³ Thus, retained traffic data in general can only be accessed upon an order from judicial authorities, or by request ‘of competent bodies for the purpose of settling disputes’.²³⁴ Retained location data can only be accessed upon order of judicial authorities.²³⁵ However, the law remains unclear as to whether ‘competent bodies’ include administrative authorities, and whether ‘disputes’ include administrative investigatory proceedings. These provisions pertain solely to the conditions for accessing data retained under the legal obligation to do so, and do not apply to data retained for other reasons, such as user consent, a legal requirement, or the necessity of processing to fulfil a contract.²³⁶

Nonetheless, the legislator has expressed a clear intention to impose specific safeguards regarding access to data, including traffic data, by ensuring prior oversight from a judicial authority or the Public Prosecutor’s Office, like in the Criminal Procedure Code. It can thus be questioned what types of data can be requested from OSPs by administrative authorities under their general powers to obtain information.

However, in absence of the interpretation of the Constitutional Court, the High Court (*Cour de Cassation*) has decided that the secret of correspondence does not protect messages of a professional nature in the context of relations between employers and employees. All correspondence exchanged using professional equipment is presumed to be professional

²³¹ Steichen, (n. 233), p. 168. Differently, the ECtHR has extended the notion of correspondence to include traffic data, which are thus protected under the right to privacy, ECtHR, *Malone v. the United Kingdom*, 02.08.1984, no. 8691/79, § 84; ECtHR, *Heglas v. Czech Republic*, 01.03.2007, no. 79650/16, § 61; ECtHR, *Copland v. the United Kingdom*, 03.04.2007, no. 62617/00, § 44.

²³² J.-L. Putz, *Cybercriminalité: criminalité informatique en droit luxembourgeois*, Luxembourg, Larcier, Regards sur le droit luxembourgeois, 2019, p. 484.

²³³ Article 4.1 of the Law on the Electronic Communications Sector, as the transposition of Article 5 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

²³⁴ Article 5.2 of the Law on the Electronic Communications Sector.

²³⁵ Article 9.2 of the Law on the Electronic Communications Sector.

²³⁶ Article 6 of the GDPR.

unless it is identified as being of a private nature.²³⁷ Extending the interpretation of that case law could enable to circumvent the protection of communications and allow access to content and traffic data of professional communications, which are particularly relevant when investigating the selected areas of enforcement.

4. TRANSFER OF DATA BETWEEN PROCEEDINGS

4.1. Transfers of data between national proceedings

In general, transfer of information between administrative sanctioning proceedings at the national level is regulated under the Law on Inter-Administrative and Judicial Cooperation.²³⁸ It enables the transfer of information either automatically, based on a secure, limited and controlled access, or upon request or spontaneously.

For example, the AEDT, the ADA and the Direct Taxes Administration can exchange information (*Administration des Contributions Directes*, ACD), upon request and for a specific case, or spontaneously.²³⁹ The AEDT and the ACD also share a common database to process information for their respective missions.²⁴⁰ The AEDT has direct access to the import/export database and road vehicle tax database of the ADA; and the ADA has direct access to the database of taxable persons for VAT purposes of the AEDT.²⁴¹ The AEDT can also exchange information with the Common Centre for Social Security, in general to assess the appropriateness of a bankruptcy petition, or specific information relevant to VAT assessment.²⁴² In that latter case, the Law on Inter-Administrative and Judicial Cooperation specifies that information should be shared electronically. Specific information is also shared by the Transport Ministry on motor vehicles to the ADA and the

²³⁷ Cour de Cassation, 15.12.2022, no. 156/2022. Analysed by J. Madert, E. Hullar, 'En matière de preuve : les bons réflexes pour un bon dossier !', *Revue Pratique de Droit Social*, 2023, vol. 18/2023, p. 25.

²³⁸ *Loi du 19 décembre 2008 ayant notamment pour objet la coopération interadministrative et judiciaire.*

²³⁹ Articles 3 and 4 of the Regulation on the Cooperation between the ACD and the AEDT (*Règlement grand-ducal du 22 janvier 2009 concernant la coopération interadministrative de l'Administration des Contributions Directes et de l'Administration de l'Enregistrement et des Domaines*). Articles 4 and 5 of the Regulation on the Cooperation between the AEDT and the ADA (*Règlement grand-ducal du 3 décembre 2009 concernant la coopération interadministrative de l'Administration de l'Enregistrement et des Domaines et de l'Administration des Douanes et Accises*).

²⁴⁰ Article 1 of the Regulation on the Cooperation between the ACD and the AEDT.

²⁴¹ Article 1 of the Regulation on the Cooperation between the AEDT and the ADA.

²⁴² Articles 8 and 9 of the Law on Inter-Administrative and Judicial Cooperation.

AEDT, in that latter case, electronically with strong authentication;²⁴³ and by the Labour Inspectorate to the AEDT, electronically.²⁴⁴ The AEDT and the Employment Development Agency can also exchange information from records and reports.²⁴⁵ The AEDT can also request information from the CSSF. Any information obtained from the CSSF must be used only for the purposes it has been transferred for.²⁴⁶ In case the information was received from a foreign competent authority, an authority of that authority is necessary to transfer the information to a different authority in Luxembourg.²⁴⁷ Tax authorities, the AEDT and the ACD, and judicial authorities, can also mutually share information.²⁴⁸

Furthermore, sectoral laws provide for rules on transfer of information between administrative authorities. The ADA can transfer information to any public entity, as long as the information is necessary for the implementation of its mission, and the transfer is in conformity with EU law. Tax secrecy shall be protected by the receiving authority.²⁴⁹ The CSSF as well as the CAA may exchange information upon several legal bases,²⁵⁰ particularly to ‘cooperate with the Government, with the Luxembourg Central bank and with other [national] prudential supervisory authorities’.²⁵¹ When receiving information, the CSSF can only use it for the purpose set in the legal basis of the transfer, unless the sending authority consent to its use for a different purpose.²⁵² Cooperation among the CSSF, the CAA and the Consignment Office is also possible, and any further transmission needs the approval of the sending authority.²⁵³

Other legal bases provide for the transfer of data between administrative and judicial authorities. Information can also be transferred between the

²⁴³ Article 14 of the Law on Inter-Administrative and Judicial Cooperation and Regulation on the Cooperation between the Transport Ministry and the AEDT (*Règlement grand-ducal du 21 mars 2024 concernant la coopération interadministrative entre le Ministère de la mobilité et des travaux publics et l’Administration de l’enregistrement, des domaines et de la TVA*).

²⁴⁴ Article 15 of the Law on Inter-Administrative and Judicial Cooperation.

²⁴⁵ Article 15^{ter} of the Law on Inter-Administrative and Judicial Cooperation.

²⁴⁶ Article 15^{quarter} §2 of the Law on Inter-Administrative and Judicial Cooperation.

²⁴⁷ Article 15^{quater} of the Law on Inter-Administrative and Judicial Cooperation.

²⁴⁸ Article 16 of the Law on Inter-Administrative and Judicial Cooperation.

²⁴⁹ Article 320 of the GLCE.

²⁵⁰ For instance, Article 8 of the Insurance Sector Law, Article 44.3 of the Law on Markets in Financial Instruments. Confidential information can only be used for the limited purposes listed at Article 11 of the Insurance Sector Law; and exchange of information to other authorities shall conform to the criteria of Article 12.

²⁵¹ Article 3-2 of the Law creating the CSSF and Article 3 of the Insurance Sector Law for the CAA. The resolution council of the CSSF can also exchange information with the Luxembourg Central Bank, Article 12-9.2 of the Law creating the CSSF.

²⁵² Article 16 of the Law creating the CSSF.

²⁵³ Article 38 of the Law on Inactive Accounts.

police and the ADA, upon judicial authorisation if the data concerns an open criminal investigation.²⁵⁴ In general, the police can transmit information to administrative authorities, upon judicial authorisation if the data is related to an open criminal investigation and when it is necessary for the implementation of the mission of the CNPD.²⁵⁵ These transmissions are controlled by the CNPD.

In general, any public authority knowing about facts that could constitute an offense must report to the Public Prosecutor's Office.²⁵⁶ As a result, various laws in the area of banking and financial markets grant the CSSF and the CAA the power to transfer information to the Public Prosecutor's office for opening a criminal prosecution.²⁵⁷ Particularly, the CSSF, the Public Prosecutor's Office and the Police 'may exchange any information they deem useful or necessary' regarding market abuse infringements.²⁵⁸ Cooperation between the CSSF and the Public Prosecutor's Office is mandatory to decide whether a specific infringement might be investigated and prosecuted in criminal or administrative proceedings. Courts can also require the Competition Authority to produce evidence from the administrative file to quantify damages.²⁵⁹

4.2. Transfers of data between foreign and national proceedings

Transfers of data between foreign and national proceedings under national law is significantly impacted by EU law. When exchanging data with third countries, this chapter will focus on national legal bases and thus exclude international and European law bases.

²⁵⁴Article 5 of the Police Exchange of Information Law (*Loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière*).

²⁵⁵ Articles 23 to 26 of the Police Exchange of Information Law.

²⁵⁶ Article 23.2 of the Criminal Procedure Code.

²⁵⁷ Law on the Financial Sector, Article 53.1.10; Law on Institutions for Occupational Retirement Provision, Article 62.1.g; Law relating to Specialised Investment Funds, Article 45.3.1; Law on Payment Services, Articles 31.4 and 58-5.1.10; Law on UCI, Article 147.2.1; Law on AIFM, Article 50.2.1; Law on Market Abuse, Article 4.1.5; Law on Payment Accounts, Article 31.5; Law on Markets in Financial Instruments, Article 45.2.8; Law on KID, Article 4.1.7, Law on Central Securities Depositories, Article 2.8; Law on Prospectuses for Securities, Articles 7.2.15° and 35.10°; Law on the Operationalisation of European Regulations in the Area of Financial Services, Articles 2.2.7, 7, 12.7, 17.2.6, 20-3.2.7, 20-9.2.8, and 20-16.2.15; Law relating to the Issue of Covered Bonds, Article 20.9°; Law on Inactive Accounts, Article 40.2.6°.

²⁵⁸ Article 7 of the Law on Market Abuse.

²⁵⁹ Article 75 of the Competition Law.

The ADA can exchange information with other EU customs authorities, which must be done through ‘electronic data-processing techniques’.²⁶⁰ Based on national law, any information to prevent and investigate infringements can be exchanged with foreign competent authorities on condition of reciprocity.²⁶¹ Furthermore, the exchange of confidential information outside of the EU customs territory can only be undertaken upon a specific legal basis, which is ‘an international agreement or Union legislation in the area of the common commercial policy’.²⁶²

The AEDT can exchange information with national competent authorities in other Member States based on Article 7 of the Council Regulation (EU) No 904/2010 of 7 October 2010 on Administrative Cooperation and Combating Fraud in the field of VAT. The request must be reasoned, and grounds for refusal are strictly limited. When the authority has already access to the information, the deadline for providing it is one month.²⁶³ The exchange of information can also occur spontaneously.²⁶⁴

Laws on the banking and financial sectors all include similar provisions on cooperation.²⁶⁵ In particular, Article 44-1 of the Law on the Financial Sector enables cooperation and exchange of information with other national competent authorities, and European supervisory bodies in the same area. The CSSF can indicate to the national authority, to which it transfers information that it cannot be further transferred or used without its express consent; the CSSF must abide to the same restriction if so requested. Grounds for refusal are limited to *ne bis in idem* issues: the existence of judicial proceedings for ‘the same actions and against the same persons before the Luxembourg

²⁶⁰ Article 6.1 of the Union Customs Code. See Commission implementing Regulation (EU) 2023/1070 of 1 June 2023 on technical arrangements for developing, maintaining and employing electronic systems for the exchange and storage of information under Regulation (EU) no. 952/2013 of the European Parliament and the Council; and Commission implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) no. 952/2013 of the European Parliament and of the Council laying down the Union Customs Code.

²⁶¹ Article 325 of the GLCE.

²⁶² Article 12 of the Union Customs Code.

²⁶³ Article 10 of Council Regulation (EU) no. 904/2010 of 7 October 2010 on Administrative Cooperation and Combating Fraud in the field of VAT.

²⁶⁴ Article 13 of Council Regulation no. 904/2010 on Administrative Cooperation and Combating Fraud in the field of VAT.

²⁶⁵ See also Articles 52 and 53 of the Law on Markets in Financial Instruments; Article 10 and 11 of the Law on Market Abuse; Article 15 of the Law on Investment Companies in Risk Capital; Article 59 of the Law on Institutions for Occupational Retirement Provision; Article 23 of the Law on Transparency Requirements; Article 33 of the Law on Payment Services; Article 134 of the Law on UCI; Articles 53 to 57 of the Law on AIFM; Articles 56 and 60 of the Law concerning the Audit Profession; Article 34 of the Law on Payment Accounts; Articles 11, 36 and 59 of the Law on Prospectuses for Securities; Article 21 of the Law relating to the Issue of Covered Bonds.

courts, or [the existence of] a final judgment [that] has already been delivered in relation to such persons for the same actions in Luxembourg'.²⁶⁶ The CSSF can also transmit information to international bodies such as the International Monetary Fund under specific conditions, or to third countries authorities based on cooperation agreements.²⁶⁷ The receiving authority must provide safeguards equivalent to the professional secrecy of the CSSF and the right to information, and guarantee purpose limitation.²⁶⁸

Based on EU law, the CSSF must also cooperate with other national competent authorities, the European Banking Authority, the European Securities and Markets Authority, and the European Insurance and Occupational Pensions Authority.²⁶⁹ The CAA can also exchange information with other EU national competent authorities, or authorities of third countries based on an agreement, as long as the professional secrecy is maintained. If information comes from another EU national authority, it can only be shared with third countries' authorities upon the express authorisation of the initial authority.²⁷⁰ The CAA can also transmit information to European supervision authorities, such as the European Securities and Markets Authority.²⁷¹ Confidential information received by the CSSF or the CAA can only be used for specific purposes, such as to impose penalties.²⁷²

The Competition Authority can exchange information with other national competent authorities, as well as with the European Commission. The information shall only be used for the purpose for which it was

²⁶⁶ Article 44-2 of the Law on the Financial Sector.

²⁶⁷ Articles 44-2a and 44-3 of the Law on the Financial Sector.

²⁶⁸ Article 44.4 of the Law on the Financial Sector.

²⁶⁹ For instance, Article 43 of the Regulation (EU) 2017/1131 of the European Parliament and of the Council of 14 June 2017 on money market funds; Article 23 of the Regulation (EU) no. 346/2013 of the European Parliament and of the Council of 17 April 2013 on European social entrepreneurship funds; Article 22 of the Regulation (EU) no. 345/2013 of the European Parliament and of the Council of 17 April 2013 on European venture capital funds; Article 35 of the Regulation (EU) no. 2015/760 of the European Parliament and of the Council of 29 April 2015 on European long-term investment funds; Article 36 of Regulation (EU) no. 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation; Article 35 of Regulation (EU) no. 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority); Articles 35 and 36 of Regulation (EU) no. 236/2012 of the European Parliament and of the Council of 14 March 2012 on short selling and certain aspects of credit default swaps. Under this text, disclosure of information to third countries requires an agreement and an express written authorisation, Article 40.

²⁷⁰ Articles 9 and 10 of the Insurance Sector Law.

²⁷¹ Articles 12 and 13 of the Insurance Sector Law.

²⁷² Article 44.6 of the Law on the Financial Sector and article 11 of the Insurance Sector Law.

requested.²⁷³ Furthermore, the authority can also exchange information, including confidential, with other competent national authority, based on the Digital Markets Act.²⁷⁴ Additionally, the Competition Authority must abide to cross-border cooperation provisions of the Law on Services in the Internal Market.²⁷⁵ This law does not apply to banking and financial, and tax services,²⁷⁶ hence its application to the CSSF, the CAA, and the AEDT is excluded. Based on this text, cross-border requests for information exchanges must be motivated and used only for the purpose they have been transferred for. Information is shared electronically.²⁷⁷

The CNPD can offer mutual assistance, including by sharing information, among national data protection authorities.²⁷⁸ Requests for information, which must be reasoned, must be answered within one month and through electronic means.²⁷⁹ Grounds for refusal are limited to lack of competence or infringement to EU or national law for compliance with the request.

4.3. Admissibility of data collected from online service providers as evidence

There are no rules on admissibility of evidence dedicated to data collected from OSPs. In general, ‘to be admitted, evidence obtained in an administrative procedure should be useful to the discovery of the truth, gathered in a fair manner and debated in an adversarial manner’.²⁸⁰ There are rare rules specific to data transferred from other (national or foreign) proceedings. Overall, they are admissible if legally obtained and duly communicated.²⁸¹ Any information obtained by a tax authority can be used by another one after its transfer.²⁸²

²⁷³ Articles 66, 73 and 74 of the Competition Law, in relation with Articles 11 and 12 of Council Regulation (EC) no. 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.

²⁷⁴ Article 38.1 of the Digital Markets Act.

²⁷⁵ *Loi du 24 mai 2011 relative aux services dans le marché intérieur, transposing Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.*

²⁷⁶ Article 1.2.b and Article 1.3 of the Law on Services in the Internal Market.

²⁷⁷ Article 25 of the Law on Services in the Internal Market.

²⁷⁸ Article 8.9° of the Law organising the CNPD.

²⁷⁹ Article 61 of the GDPR.

²⁸⁰ K. Ligeti, S. Tosza, ‘Admissibility of Evidence, Transnational E-Evidence and Fair-Trial Rights in Luxembourg’, in: L. Bachmaier Winter, F. Salimi (eds.), *Admissibility of evidence in EU cross-border criminal proceedings: electronic evidence, efficiency and fair trial rights*, Hart Publishing, Hart studies in european criminal law, 1st ed., 2024, p. 98.

²⁸¹ *Ibid.* p. 94.

²⁸² Articles 3 and 6 of the Law on Inter-Administrative and Judicial Cooperation.

Generally, Luxembourg administrative and criminal proceedings are based on the principle of freedom of proof. In front of administrative courts, the evidence only needs to be brought to the case through a deposit at the tribunal's registry, and then be communicated to the parties, to respect the adversarial principle.²⁸³ The evidence must be licit, meaning that it should have been collected in accordance with legal provisions and the principles of the fair trial.

According to the Luxembourg case law, illicit evidence can be discarded only 'if certain formal conditions had to be met on penalty of nullity and the irregularity affected the credibility of the evidence', or in case of a violation of the right to a fair trial (especially of the adversarial principle).²⁸⁴ This case law was issued in the context of criminal proceedings, which provides for more formal conditions for applying its coercive measures.²⁸⁵ If it was to apply to administrative (or civil, in case of VAT) judicial proceedings, it would find very little application as very few formal conditions are prescribed under the penalty of nullity in those proceedings.²⁸⁶

Some sectoral laws provide additional information regarding admissibility of evidence. Admissible evidence in front of the Competition Authority encompasses all 'documents, oral statements, electronic messages, recordings and any other items containing information, regardless of form or medium'.²⁸⁷ Any information or document obtained by the AEDT may be

²⁸³ Article 8 of the Law on Proceedings before Administrative Courts (*Loi du 21 juin 1999 portant règlement de procédure devant les juridictions administratives*).

²⁸⁴ S. Menetrey, 'Preuve et droits fondamentaux en droits européen et luxembourgeois', in: Collectif (ed.), *Annales du droit luxembourgeois 2013*, Bruxelles, Bruylant, *Annales du droit luxembourgeois*, 2015, p. 33, analysing Cour de cassation, 22.11.2007, no. 57/2007. See also K. Ligeti, 'Luxembourg', in: F. Giuffrida, K. Ligeti (eds.), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, University of Luxembourg, 2019, p. 187.

²⁸⁵ In criminal proceedings, a nullity request must be filled in front of the pre-trial chamber of the district court within five days when obtaining knowledge about the act, Articles 48-2 (preliminary investigation) and 126 (instruction) of the Criminal Procedure Code. See V. Covolo, 'Luxembourg', in: S. Allegrezza, V. Covolo (eds.), *Effective Defence Rights in Criminal Proceedings. A European and Comparative Study on judicial remedies*, Wolters Kluwer Italia, 2018, pp. 365-366.

²⁸⁶ The admissibility of evidence is mainly not addressed by the competent administrative authorities, and such a topic must be discussed in front of courts, whenever the decision is open for judicial review. Furthermore, due to the autonomy of criminal law, the inadmissibility of evidence in administrative proceedings does not impact the same assessment in criminal proceedings where the same evidence is used. Similarly, criminal proceedings and tax proceedings are independent regarding the assessment of the admissibility of evidence, Ligeti, (n. 282), p. 192.

²⁸⁷ Article 20.2 of the Competition Law.

invoked by the State for the recovery of any sum due under tax laws.²⁸⁸ Information obtained by the AEDT will not be controlled but will be admissible as evidence according to the records of its agents.²⁸⁹ Records of judicial police officers, customs officers, and law enforcement officers responsible for assisting with tax inspections are also admissible.²⁹⁰ However, oath cannot be used as proof under tax proceedings in front of the AEDT and administrative judges.²⁹¹

5. CONCLUSION

Powers to request data, meaning, electronic information, from OSPs in punitive administrative proceedings are limited to three sectoral frameworks enforced by the CSSF. These are also the only cases where an administrative authority must request a judicial authorisation. Nevertheless, administrative authorities generally have broad powers to request any information, including stored electronically, from any persons. The ECJ case law, in particular regarding enforcement of the legislation on financial markets and of data protection, supports extended interpretation of these texts. Despite the opportunities to gather useful information from OSPs for administrative proceedings, the interviews conducted with practitioners in Luxembourg highlighted that ADA and the CSSF usually do not have the necessity to do so. Investigative powers of the CNDP to obtain information from third parties, despite being not enforceable (see section 3.1.5), still face generally unquestioned compliance: ‘companies feel *de jure*, or at least *de facto*, obliged to cooperate, and are reluctant to seek redress’.²⁹² Finally, third parties, such as OSPs, can voluntarily provide information to national authorities such as the Competition Authority.²⁹³

It seems clear that the scope of these powers has not yet taken into account the opportunities (and challenges) brought by the possibility to acquire electronic evidence from OSPs.²⁹⁴ Furthermore, the new Constitution

²⁸⁸ Article 70.2 of the VAT Law, referring to Article 31 of the Law to Ensure the Fair and Accurate Collection of Registration and Inheritance Taxes (*Loi du 28 janvier 1948 tendant à assurer la juste et exacte perception des droits d'enregistrement et de succession*).

²⁸⁹ Article 68§1 of the VAT Law.

²⁹⁰ Article 68§3 of the VAT Law.

²⁹¹ Article 59.3 of the Law on Proceedings before Administrative Courts and article 68 of the VAT Law.

²⁹² J.-L. Putz, *Données personnelles et droit pénal*, Legitech, Bibliothèque de la Revue Pénale Luxembourgeoise, 2024, p. 25.

²⁹³ Article 27.1 of the Digital Markets Act.

²⁹⁴ See S. Tosza, ‘European Union · The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?’, *European Data Protection Law Review*, 2023, vol. 9, no. 2, pp. 163-172; S. Tosza, ‘Mutual Recognition By Private Actors In Criminal Justice? E-

requires taking into account the inviolability of communications, together with the Law on the Electronic Communications Sector. It is not clear whether the constitutional rights concern the protection of traffic data, while the sectoral law clearly indicates the will of the legislature to ensure judicial oversight of access to data, including traffic data. While electronic evidence could become an asset to investigate administrative infringements, no less than for criminal investigations, the legal framework is sparse and clearly lacks consistency.

Safeguards against investigatory powers of administrative authorities suffer from the same shortcomings. The general framework on administrative proceedings remains vague, framed into principles recognised and detailed by the case law. Although OSPs could face non-negligible sanctions when not answering properly to a request for data of an administrative authorities, there are few to no remedies dedicated to third parties. The consequences of such situation are exacerbated as a request for data is usually not interpreted as an administrative decision, and thus, no safeguards nor remedies are available.

11. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN THE NETHERLANDS

*A. DE VRIES, L. MUSTERT, M. LUCHTMAN, A. DUIJKERSLOOT, and R.
WIDDERSHOVEN*

Dutch authorities have various supervisory powers to implement their enforcement tasks. These powers allow the authorities to gather information to establish whether the applicable substantive rules are complied with by natural and legal persons and, if not, take measures to address breaches of those rules, including the imposition of punitive administrative sanctions. Increasingly, Dutch administrative authorities rely on their supervisory powers to obtain digital information, including from ‘third parties’ such as online service providers (OSPs). In this contribution, we assess the applicable framework regarding the gathering of data as evidence in punitive administrative proceedings in the Netherlands, with a specific emphasis on the options and limits of obtaining such evidence from OSPs and the sharing and use of such evidence at the interface of administrative and criminal enforcement.

1. COMPETENT AUTHORITIES IN SELECTED AREAS OF PUNITIVE ADMINISTRATIVE ENFORCEMENT

In this Section, we will present an overview of some relevant characteristics of the selected administrative authorities: the Dutch Tax Administration (*Belastingdienst*) and Customs Administration (*Douane*), the Authority for the Financial Markets (*Autoriteit Financiële Markten*, AFM), the Authority for Consumers and Markets (*Autoriteit Consument en Markt*, ACM), and the Data Protection Authority (*Autoriteit Persoonsgegevens*, AP).

As a preliminary remark, we draw attention to the so-called dual enforcement system in the Netherlands. Since the early 1990s, criminal and punitive administrative enforcement have existed side by side in many policy fields. Breaches of substantive legislation often amount to both a criminal and an administrative offence. The Dutch Public Prosecution Service (*Openbaar Ministerie*, OM) has retained a monopoly to prosecute criminal offences

before courts. In turn, various administrative authorities across numerous policy fields have been awarded the competence to impose administrative fines – which constitutes a punitive sanction based on national law – for administrative offences. In several cases, the Dutch legislator accepts both enforcement tracks, leaving the final decision on the appropriate allocation to the administrative and judicial authorities involved. In the subsequent overview of the aforementioned administrative authorities' characteristics, we will also refer briefly to this 'duality' aspect.

1.1. Customs and tax (VAT) enforcement

The Douane and the Belastingdienst constitute Directorates-General resorting under the Ministry of Finance.¹ The Douane is charged with the enforcement of customs legislation, in particular the Dutch General Customs Act (ADW) and the Union Customs Code (UCC), including the applicable prohibitions and limitations to cross-border movements of goods. The Belastingdienst enforces VAT law, especially the EU VAT Directive 2006 and the transposing laws, in particular the Law on Turnover Tax 1968 (Wet OB).

In cases of designated infringements of customs and tax (VAT) law, the Tax Inspector can impose an administrative fine or a fiscal penalty order (see Section 2.1).² In serious cases, the criminal investigation will be transferred to the Fiscal Information and Investigation Service (*Fiscale Inlichtingen- en Opsporingsdienst*, FIOD). The FIOD constitutes a so-called 'special investigation service', and while it is institutionally part of the Belastingdienst, it will function under the auspices of the OM during criminal investigations and has judicial tasks.³ The FIOD is charged with the investigation of tax fraud and miscellaneous forms of financial-economic crime, including the investigation of customs offences.

1.2. Enforcement in the area of financial markets

The AFM constitutes a foundation on the basis of civil law that has its registered office in Amsterdam. It is an independent administrative body with legal personality. It is established in the Financial Supervision Act (Wft) that the AFM is charged with market conduct supervision.⁴ The supervisory tasks

¹ This organisational structure can be found in the Implementing Regulation Tax and Customs Administration 2003 (*Uitvoeringsregeling Belastingdienst 2003*, Urb 2003).

² Article 9:1 *Wet op de Omzetbelasting 1968* (Wet OB) and Article 10:15 *Algemene douanewet* (ADW).

³ Article 3(1)(d) Urb 2003.

⁴ Article 1:25(2) *Wet op het financieel toezicht* (Wft).

of the AFM extend to many national and European rules.⁵ If the AFM identifies breaches of the aforementioned rules, it has various administrative sanctions at its disposal.⁶ These sanctions may have a non-punitive (reparatory) or a punitive character.⁷ The administrative fine is a punitive sanction (see Section 2.1.). Some infringements may constitute a criminal offence and may be prosecuted by the OM. For example, this is the case with serious instances of market abuse.⁸

1.3. Competition law enforcement

The ACM – located in The Hague – is responsible for general competition supervision in the Netherlands, but also the protection of consumer rights and the regulation of (parts of) the energy, telecommunications, postal and transport markets. The establishment of the ACM is regulated in the Consumer and Markets Authority Establishment Act. According to this act, the ACM aims to promote well-functioning markets, orderly and transparent market processes and careful treatment of consumers. This means monitoring, promoting and protecting effective competition and equal competitive conditions on markets and removing obstacles to this.⁹ The following regulations are particularly relevant regarding the enforcement of competition law: the ACM Establishment Act, the Competition Act (Mw), Regulation 1/2003 and Directive 2019/1.¹⁰ They form the basis for the ACM's supervisory and sanctioning powers.

⁵ Such as the Audit Firms Supervision Act, the Pension Act, the Consumer Protection Enforcement Act, the Prevention of Money Laundering and Terrorist Financing Act, Regulation (EU) No 596/2014 on market abuse (the MAR), the (revised) Directive on Markets in Financial Instruments (the MIFID II), the Packaged Retail and Insurance-based Investment Products Regulation (the PRIIPS), and the Markets in Crypto-Assets regulation (the MICAR).

⁶ See Articles 1:75-1:88a Wft.

⁷ Non-punitive sanctions that can be used are instructions or public warnings, placing institutions under undisclosed custody, withdrawing licenses, cancelling or refusing registrations and periodic penalty payments. The non-punitive character of some of these sanctions might be food for discussion. See A. Duijkersloot and R. Widdershoven, 'Administrative law enforcement of EU law' pp. 42-43, in: M. Scholten (ed), *Research Handbook on the Enforcement of EU Law*, Cheltenham, United Kingdom, Edgar Elgar Publishing, 2023.

⁸ Article 1 Dutch Economic Offences Act (*Wet op de economische delicten*, WED) and Articles 14 and 15 MAR.

⁹ Article 2(5) ACM Establishment Act.

¹⁰ *Mededingingswet* (Mw); Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty; Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market.

Sanctioning of violations of competition law only takes place under administrative law. The powers to impose those sanctions are laid down in substantive legislation, for competition law, in particular, the Mw. Infringements of the competition rules can be sanctioned with a periodic penalty payment (reparatory) and the punitive sanction of the administrative fine (see Section 2.1.).¹¹

1.4. GDPR enforcement

The AP – located in The Hague – has been established and designated as the supervisory authority regarding compliance with data protection rules, particularly the GDPR and the GDPR Implementation Act (UAVG). The AP constitutes an independent administrative body with legal personality.¹² The main tasks and powers of the AP are listed in Articles 57 and 58 of the GDPR. The tasks comprise supervision, providing advice on, *inter alia*, legislative proposals, providing information on, amongst others, the interpretation of personal data protection legislation, and international assignments, such as cooperation with other supervisory authorities concerned to address transnational GDPR infringements when the AP is the lead supervisory authority.¹³ The powers are subdivided into investigative powers, corrective powers, and authorisation and advisory powers.¹⁴

The corrective or sanctioning powers can be of a non-punitive (reparatory) nature, such as the powers to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of the GDPR and to order the controller or the processor to comply with the data subjects' requests to exercise their rights pursuant to the GDPR. The Dutch legislator has made use of the possibility under the GDPR to grant additional powers and has included in the UAVG the power to impose an administrative enforcement order. This implies that the AP can impose a periodic penalty payment as well.¹⁵ Punitive sanctions are also available to the AP, in particular the power to impose administrative fines.¹⁶ The UAVG does not foresee criminal law enforcement.

¹¹ Article 56 Mw. Other possible sanctions are behavioural or structural remedies and interim measures, see Article 58a and 58b Mw. These are variations on the periodic penalty payment, which have been textually adapted since Directive 2019/1.

¹² Article 6(1) *Uitvoeringswet Algemene verordening gegevensbescherming* (UAVG).

¹³ Article 57(1) GDPR.

¹⁴ Article 58(1)-(3) GDPR.

¹⁵ Article 5:32(1) Awb.

¹⁶ Articles 58 j and 83 GDPR.

2. PUNITIVE ADMINISTRATIVE PROCEEDINGS: GENERAL FRAMEWORK

Since 1994, the General Administrative Law Act (Awb) has featured an overarching procedural framework for administrative proceedings. The Awb provides, *inter alia*, the definitions of the main concepts of Dutch administrative law, the general principles of good administration that govern administrative action, the general rules of administrative procedure, including on administrative review procedures, the rules on judicial review, the powers that are available to administrative authorities and their officials, and the definitions and rules on administrative sanctions. Notably absent from the Awb are rules on international and European mutual administrative assistance with authorities from other (Member) States or EU agencies.¹⁷

Although the Awb establishes an overarching legal framework, sectorial legislation remains relevant. Sectorial legislation often features additional or diverging rules compared to the *lex generalis*, specifically geared towards the relevant substantive policy field. Moreover, the Awb does not apply to several policy fields, most notably in tax and customs matters. The State Taxes Act (AWR) and General Customs Act (ADW) explicitly provide that tax and customs proceedings are governed by tailored rules of the AWR and ADW instead.¹⁸

2.1. Administrative sanctions under Dutch law, particularly the administrative fine

The Awb provides an overarching procedural framework for two kinds of administrative sanctions: the ‘reparatory sanction’ and the ‘punitive sanction’. The reparatory sanction has a reparatory and preventive aim: it strives to rectify or end, wholly or in part, a violation, to prevent the repetition of a violation, or to remove or limit the consequences of a violation. In turn, the punitive sanction is an administrative sanction that aims at adding harm to the offender.¹⁹ The administrative fine is the most relevant sanction modality under Dutch administrative law for this contribution. The

¹⁷ In this context, see e.g. A. de Vries, *Evidence and Transnational Punitive Enforcement Proceedings in the European Union*, The Hague, Netherlands, Eleven, 2024, pp. 219 and followings. The Dutch legislator did consider the option of providing a general framework on mutual administrative assistance in the Awb but decided to leave the matter to sectorial legislation in the end, see P. Boswijk, O. Jansen and R. Widdershoven, ‘De wettelijke implementatie van administratieve samenwerking in de Europese Unie’ *Regelmaat*, 2009, p. 323.

¹⁸ See, e.g., Article (1)3 AWR (*Algemene wet inzake rijksbelastingen*) and Article 1:6 ADW.

¹⁹ Article 5:2(1)(c) Awb. According to the Administrative Law Division of the Council of State, ‘harm’ constitutes inflicting detriment beyond that which results from the mere enforcement of the regulation imposed by or under the law, see ABRvS 19.09.1996, ECLI:NL:RVS:1996:ZF2322.

administrative fine – which entails the unconditional obligation to pay a sum to an administrative authority – is the only punitive sanction defined and regulated in the Awb.²⁰ While the Awb provides the general overarching procedural framework concerning the available administrative sanctions, the competence to impose such sanctions is awarded based on sectorial legislation. An administrative fine is imposed through a decision taken by an administrative authority.

To ‘investigate’ offences for which an administrative fine can be imposed, Dutch administrative authorities can rely upon various supervisory powers in accordance with the Awb or sectorial legislation (see also Section 3). These powers under administrative law are identical for the ‘regular’ (monitoring) measures taken by administrative authorities to ensure compliance with policies which do not require indications of breaches of these policies, and administrative proceedings to impose reparatory and/or punitive sanctions.²¹ Therefore, what sets the so-called ‘administrative investigation to impose an administrative fine’ (*boeteonderzoek*) apart from monitoring and non-punitive administrative enforcement proceedings is not the available supervisory powers, but rather the applicable procedural safeguards that can be invoked by the person concerned (see also Section 2.3).²² The administrative fine qualifies, according to the literature, as a ‘penalty of a criminal nature’ under EU law and a ‘criminal charge’ within the meaning of Article 6 of the European Convention on Human Rights (ECHR).²³

In accordance with the Awb, the ‘administrative penalty payment’ and ‘administrative enforcement order’ constitute reparatory sanctions. In fiscal matters, the ‘additional tax assessment’ (tax matters) and ‘invitation to pay’ (customs) are also considered to have a reparatory character, but they are not governed by the Awb. Although non-punitive administrative proceedings are, in principle, outside the scope of this Chapter, the aforementioned measures are essential enforcement tools for the administrative authorities and are often applied parallel to or as an alternative to an administrative fine (or criminal law enforcement). Furthermore, they may be used to enforce the obligation to cooperate with the authorities (see Section 2.2.1).

²⁰ Article 5:40 Awb. See F. Michiels, A. Blomberg and G. Jurgens (eds), *Handhavingsrecht*, Deventer, Netherlands, Kluwer, 2016, p. 101.

²¹ In this context, see A. Blomberg, ‘Handhaving en toezicht’, pp. 33-35, in: F. Michiels and E. Muller (eds), *Handhaving. Bestuurlijk handhaven in Nederland*, Deventer, Netherlands, Kluwer, 2013; L. Rogier, ‘Toezicht op de naleving in de Algemene wet bestuursrecht’, p. 3, in: L. Rogier and H. de Doelder (eds), *Toezicht. Opstellen over veiligheidstoezicht en markttoezicht*, The Hague, Netherlands, Boom juridische uitgevers, 2006. See also De Vries (n. 17) pp. 180-181.

²² Michiels, Blomberg and Jurgens (n. 18) pp. 20-21 and 44 and followings.

²³ Ibidem, pp. 102-103.

2.2. Competences to gather data as evidence under Dutch administrative law

The Awb establishes the general framework for administrative proceedings, including administrative powers that can be relied upon by the officials of administrative authorities to gather evidence. The Awb does not feature ‘digital-specific’ powers. Instead, the ‘regular’ administrative powers are relied upon to obtain both ‘analogous’ and digital evidence.

2.2.1. The supervisory powers in the General Administrative Law Act

The Awb awards supervisory powers to the ‘supervisor’ (*toezichthouder*). The supervisor is a natural person who is charged by, or pursuant to, a statutory provision with monitoring compliance with substantive rules under, or pursuant to, a statutory provision.²⁴ The Awb does not decide who are ‘supervisors’; that is established by, or in accordance with, sectorial legislation. The exercise of supervisory powers by the supervisor is determined by unwritten general principles of good administration as well as statutory law. First and foremost, the supervisor should only rely upon their powers in so far that is reasonably required for the performance of their statutory duties.²⁵ In particular, the supervisor must adhere to the principles of proportionality and subsidiarity when implementing their statutory tasks, and powers must only be used in the policy field wherein the supervisor is competent. Compliance with statutory law and general principles, including observance of fundamental rights, is reviewed when the exercise of supervisory powers is, directly or indirectly, subjected to judicial scrutiny (see Section 3.5).²⁶

We focus our analysis on two supervisory powers, provided in the Awb, that are most relevant for gathering digital evidence: the power to require anyone to provide information to the authorities, and the power to inspect all business documents and records. We also discuss the power to access professional locations and perform an on-the-spot inspection. It must be noted that the aforementioned powers are often available based on sectorial legislation in policy fields to which the Awb does not apply, for example in tax matters.²⁷

The Awb provides that a supervisor is competent to demand information from anyone and inspect all business documents and records.²⁸ In practice,

²⁴ Article 5:11 Awb. See Michiels, Blomberg and Jurgens (n. 20) pp. 21-22.

²⁵ Article 5:13 Awb.

²⁶ Michiels, Blomberg and Jurgens (n. 20) pp. 42-43.

²⁷ Article 47 AWR.

²⁸ Articles 5:16 and 5:17 Awb.

the demarcation between these two powers is opaque – especially when data is concerned – since they both concern the (direct or indirect) exchange of information from a party to the administrative authorities.²⁹

The power to demand information from anyone allows the supervisor to question persons and/or demand the surrender of relevant documents.³⁰ The statutory wording of the power shows that a demand for information can be made against anyone, including the person concerned. For this Chapter, it should be noted that a demand for information can also be made against third parties that hold relevant information, such as OSPs. A demand for information can be made verbally (on the spot) but is usually done in (digital) writing.

The power to inspect business documents and records enables the supervisor to examine, *inter alia*, the bookkeeping, administration, maintenance reports, and transport reports.³¹ The term ‘records’ is broad and covers data – including GPS registrations, email data, mailboxes, USBs – as well.³² As was the case regarding the power to demand information, the power to inspect business documents and records can be applied to anyone, including third parties such as OSPs. However, this possibility may be limited by the supervisor’s obligation to adhere to the principles of proportionality and subsidiarity. In a judgment from the Central Appeals Tribunal from 2018 concerning social security benefits, it was considered to be a violation of the principles of proportionality and subsidiarity that an administrative authority

²⁹ See O. Jansen, *Het handhavingsonderzoek. Behoren het handhavingstoezicht, het boeteonderzoek en de opsporing verschillend te worden genormeerd? Een interne rechtsvergelijking*, Nijmegen, Netherlands, Ars Aequi Libri, 1999, p. 18. In practice, the precise distinction between the power to demand information and the power to inspect business documents and records is not too important, because most officials are awarded both powers on the basis of the Awb. If this is different in accordance with sectorial legislation, problems can arise. An illustration can be found in the powers of officials of the AFM. In accordance with Article 1:74 Wft, officials are *only* awarded the power to demand information; the power to inspect documents and records and to make copies of them is *not* mentioned. Does this mean that officials of the AFM cannot inspect and copy documents? Such an outcome could lead to problems, especially in light of several instruments of EU secondary law – e.g., the now-replaced Directive 2004/39/EG (MIFID) – that require that officials of the AFM should be able to inspect documents and make copies. It has been recognised in Dutch case law that consistent interpretation implies that the power to demand information also covers the power to make copies of the information obtained, see CBb 21.09.2015, ECLI:NL:CBB:2015:288. Under the Awb, such problems will not arise because both powers are attributed to supervisors. In this context, see O. Jansen, ‘Koudwatervrees in een bananenkoninkrijk? Over de toekomstbestendigheid van titel 5.2 Awb’ *JBPlus*, 2017, 0, § 3.

³⁰ Michiels, Blomberg and Jurgens (n. 20) p. 32.

³¹ *Ibidem*, pp. 33-34.

³² *Ibidem*, p. 34.

had demanded an individual's banking statements from the bank (a third party) and had not demanded this information from the individual *first*.³³

The supervisor cannot merely inspect business documents and records but is also allowed to make copies, including so-called 'forensic copies' of data.³⁴ It is not allowed to seize documents and records; they must be returned after copies have been made. Personal documents or, in a broader sense, non-business documents cannot be inspected and/or copied. This also applies to business documents covered by legal professional privilege (see Section 2.3.1). The Awb does not prescribe how administrative authorities should guarantee that personal documents or documents covered by legal professional privilege should be 'filtered' from the materials obtained by the administrative authorities. Instead, several Dutch administrative authorities have adopted their own practice for their specific policy field(s) (see Section 3).

The power of the supervisor to access professional locations and perform an on-the-spot inspection has an 'indirect relevance' for this contribution as it enables the supervisor to access professional locations – including, at least in theory, the premises of OSPs – to rely on the two aforementioned powers (demand information, inspection of business documents and records) as part of the on-the-spot inspection. The supervisor can bring technical equipment and be accompanied by experts or other officials, including foreign officials.³⁵ The power to enter professional premises allows the supervisor to 'look around' after entering; a supervisor cannot conduct a 'search' under Dutch general administrative law, although exceptions to this rule may apply based on sectorial legislation.³⁶ The Awb does not provide the power to access and inspect *private* premises, including dwellings. In this light, a supervisor can only enter dwellings if the occupant provides their 'informed consent'.³⁷

An important characteristic of Dutch administrative proceedings is the duty to cooperate with the authorities: *anyone* is held to provide all cooperation that can reasonably be demanded in the performance of statutory

³³ CRvB 11.10.2018, ECLI:NL:CRVB:2018:3205.

³⁴ Michiels, Blomberg and Jurgens (n. 20) pp. 35-36.

³⁵ Article 5:15(3) Awb.

³⁶ Michiels, Blomberg and Jurgens (n. 20) p. 25. In Dutch doctrine, the inspection of the premises and all materials that can be seen by the supervisor without taking further action amounts to 'looking around'. Actions that aim to discover documents or other materials that are hidden from plain sight constitute a 'search'.

³⁷ Ibidem, pp. 26-27. If such consent is not obtained, the dwelling cannot be entered; Dutch administrative law does not foresee that a dwelling is entered against the will of the occupant through a warrant, although this is sometimes different in accordance with sectorial legislation.

duties to the supervisor.³⁸ The duty to cooperate also applies in tax and customs matters.³⁹ It can be concluded that the duty to cooperate applies to the person concerned and miscellaneous persons, including third parties such as OSPs. Thus, OSPs are held to provide the data to the authorities when required to do so. The refusal or failure to comply with demands by the supervisor constitutes a criminal offence threatened with a custodial sentence (three months) or a fine (maximum 5.150 euros). Moreover, the obligation to cooperate with the supervisor can be enforced through an administrative enforcement order or a periodic penalty payment.⁴⁰ In addition, a failure to comply may lead to an administrative fine being imposed based on sectoral legislation in some policy areas.⁴¹

2.2.2. Questions on the gathering of digital evidence in accordance with administrative law

When the Awb was introduced in the 1990s, the Dutch legislator decided that the available supervisory powers for administrative authorities should remain limited in scope and few in number. The idea was that the authorities did not need far-reaching powers of ‘investigation’ as their punitive enforcement task would be reserved for small and uncomplicated breaches of substantive rules.⁴² Intrusive investigative powers were restricted to criminal proceedings *sensu stricto*.⁴³ Furthermore, the catalogue of supervisory powers was primarily geared towards the gathering of ‘classic’ (physical) evidence, not data. The present reality is, however, different from the 1990s when it concerns the role of punitive administrative enforcement, and the specific requirements and concerns – especially on the observance of fundamental rights – of the gathering of data as evidence.

³⁸ Article 5:20 Awb.

³⁹ Articles 47 AWR and 1:5 ADW.

⁴⁰ Article 5:20(3) Awb.

⁴¹ Criminal penalties and the imposition of an administrative fine cannot accumulate with regard to the same offence. That would be at odds with the principle of *ne bis in idem* and the so-called ‘una via’ principle enshrined in Dutch law (Articles 5:44 Awb and 243(2) *Wetboek van Strafvordering* (WvSv)). ‘Punitive’ sanctions under criminal or administrative law and ‘reparatory’ sanctions can accumulate without triggering the principle of *ne bis in idem*. Of course, the imposition of several criminal or punitive administrative penalties for the same offence is also prohibited.

⁴² In this context, see also J. Crijns and M. van Emmerik, ‘Legaliteit van onderzoeksbevoegdheden in het bestuursstrafrecht’, pp. 239-240, in: B. van der Vorm (ed), *Bestuursstrafrechtspleging*, The Hague, Netherlands, Boom juridisch, 2024.

⁴³ *Kamerstukken II* 1993/94, 23700, No 3, 137; *Kamerstukken II* 1994/95, 23700, Nr 5, 50 and 82. See also Jansen, ‘Koudwatervrees in een bananenkoninkrijk? Over de toekomstbestendigheid van titel 5.2 Awb’ (n. 29) § 4; M. Venderbos, ‘De normering van bestuurlijk toezicht- en controleonderzoek’ *JBPlus*, 2019.

Over the years, punitive administrative enforcement in the Netherlands has far outgrown the ‘limited’ role envisioned for it, both in scale and severity of the penalties. Administrative fines constitute an important (even primary) means of punitive enforcement in many substantive policy fields, and the applicable maximum fines are – often in accordance with EU legislation – very high. Furthermore, technological progress has made data a crucial source of information and evidence for administrative authorities. By extension, administrative authorities require appropriate supervisory powers to obtain such data so that they can perform their enforcement tasks effectively. Thus, questions can be raised on how ‘future-proof’ the current general framework of the Awb is.⁴⁴

Furthermore, Dutch courts have in recent years been required to rule on the lawfulness of digital supervision techniques deployed by administrative authorities to gather evidence for reparatory measures and/or administrative fines. Various administrative authorities have relied upon far-reaching and intrusive techniques to perform their statutory duties, often citing the ‘general’ powers from the Awb or sectorial legislation as the applicable legal basis.⁴⁵ In several cases, Dutch courts have ruled that using such techniques was unlawful and, therefore, the evidence obtained had to be excluded. In those judgements, the intrusiveness of the techniques and the requirements of the legality principle and Article 8 ECHR play a decisive role: intrusive digital techniques that lead to serious interference with the right to private life require a distinct legal basis instead of the ‘general’ powers. For example, systemic surveillance through a GPS tracker on a car and covert camera surveillance on professional premises or dwellings have been found to lack a legal basis in administrative law and, therefore, constitute a violation of Article 8 ECHR.⁴⁶ Similarly, the Dutch Supreme Court ruled that the use by the Tax Administration of automatic number plate recognition (ANPR) data collected by the Dutch police was unlawful, because there was no specific legal basis that allowed the Tax Administration to request such data from the police.⁴⁷ In its ruling, the Supreme Court explicitly considered that ANPR data was systematically collected, recorded, edited and stored for years, and allowed the detailed mapping of the movement of individual vehicles, leading to a

⁴⁴ See R. Klein, S. Nuijten and X. Born, ‘Controlebevoegdheden. Verslag VAR-studiemiddag 25 juni 2015’ *NTB*, 2015, pp. 330-337; Jansen, ‘Koudwatervrees in een bananenkoninkrijk? Over de toekomstbestendigheid van titel 5.2 Awb’ (n. 29) §0; G. Roth and L. Hillen, ‘Digitaal onderzoek door de AFM. Hoe gaat dat in zijn werk, mag dat zomaar en hoe adequaat is de rechtsbescherming’ *Ondernemingsrecht*, 2020, p. 778.

⁴⁵ Venderbos, ‘De normering van bestuurlijk toezicht- en controleonderzoek’ (n. 43) § 1.3.

⁴⁶ CRvB 13.09.2016, ECLI:NL:CRVB:2016:3479; CRvB 15.03.2016, ECLI:NL:CRVB:2016:947. See also CRvB 20.12.2022, ECLI:NL:CRVB:2022:2792.

⁴⁷ HR 24.02.2017, ECLI:NL:HR:2017:286.

serious interference with the right to private life.⁴⁸ The sharing of such information needs a specific legal basis; the general competence to request information did not suffice.

2.2.3. Intrusive investigative powers and Dutch criminal proceedings

While this contribution takes the perspective of gathering of data, especially from OSPs, in punitive administrative proceedings, some considerations about the gathering of such data in criminal proceedings are warranted. The reason for this is two-fold. As mentioned previously, intrusive – often covert – investigative measures are, in principle, reserved to criminal proceedings *sensu stricto* in accordance with Dutch doctrine. This means that the gathering of data as evidence through such measures is, first and foremost, possible in the context of a criminal investigation. Secondly, data obtained in criminal investigations – including data obtained from OSPs – can later be transferred to the administrative authorities and used to impose, *inter alia*, administrative fines (see Section 4.1.2.).

A criminal investigation is pursued under the auspices of the public prosecutors of the Dutch Public Prosecution Service in accordance with the rules of the Dutch Code of Criminal Procedure (WvSv).⁴⁹ The public prosecutor can order any OSP to surrender data concerning a subscriber as well as the traffic and location data of this subscriber.⁵⁰ While statutory law does not require that prior judicial authorisation is obtained before a demand to surrender traffic and location data is made, the Supreme Court has recently adopted a consistent interpretation of the Dutch provisions on the surrender of traffic and location data in line with the judgement of the Court of Justice in *Prokuratuur* which does require prior judicial authorisation.⁵¹

⁴⁸ HR 24.02.2017, ECLI:NL:HR:2017:286, para 2.3.2-2.3.3.

⁴⁹ Several specialised investigative services (*bijzondere opsporingsdiensten*) exist in the Netherlands that are charged with conducting criminal investigations into tax and financial offences or other forms of crime relating to social-economic or environmental policies, see J. Nelen, 'De bijzondere opsporingsdiensten' in F. Michiels and E. Muller (eds) (n. 21) pp. 297-298. The special investigative services operate under the supervision of public prosecutors attached to the Public Prosecution Service Office for Financial, Economic and Environmental Offences (Articles 148b and 9(3) WvSv). For this contribution, the FIOD is the most important investigative service as it is charged with criminal investigations into fraud and other tax and financial offences. See also De Vries (n. 17) p. 169.

⁵⁰ Article 126n WvSv.

⁵¹ G. Corstens, M. Borgers and T. Kooijmans (eds), *Het Nederlandse strafprocesrecht*, Deventer, Netherlands Kluwer, 2018, p. 523. See also ECJ, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*, 02.03.2021, C-746/18; HR 05.04.2022, ECLI:NL:HR:2022:475. It is mandatory for the public prosecutor to obtain a

2.3. Defence rights under Dutch administrative law

During the gathering of data to impose an administrative fine, Dutch administrative authorities must comply with national and European fundamental rights standards, including the right to a fair trial. Because the administrative fine qualifies as a ‘punitive sanction’ under Dutch administrative law and a ‘penalty of a criminal nature’ and ‘criminal charge’ on the basis of EU law and Article 6 ECHR, several ‘criminal’ defence rights apply. For this contribution, we focus on the legal professional privilege, but we also briefly address the right to silence and privilege against self-incrimination.

2.3.1. Legal professional privilege

Under Dutch law, lawyers are held to observe confidentiality and secrecy regarding the information they receive in their professional capacity. The legal professional privilege is closely connected to this obligation: all information exchanged between the lawyer and his client in their respective capacities is protected, and the lawyer cannot be required to communicate this information to the authorities verbally or in writing.⁵² It also follows from the legal professional privilege that enforcement authorities are not allowed to consult documents or files (including digital files located on computers or smartphones) which comprise information that falls under the legal professional privilege (see also Section 3). The legal professional privilege

warrant from the investigative judge – which, of course, is an important safeguard to ‘counterbalance’ the intrusive nature of the measure – prior to requiring the surrender of traffic and location data; subscriber data can be required without a warrant.

⁵² In the Netherlands, the legal professional privilege can be invoked by both ‘independent’ and ‘in-house’ lawyers. The Supreme Court has accepted this rule in civil and criminal matters but due to its qualification as a general principle of law, the scope of the professional legal privilege should – in our view – be identical in administrative proceedings, see See HR 01.03.1985, ECLI:NL:HR:1985:AC9066; HR 13.03.2013, ECLI:NL:HR:2013:BY6101; HR 24.05.2022, ECLI:NL:HR:2022:760. In-house lawyers will only be able to invoke their privilege if guarantees (ie, a professional statute which specifies the relationship between the employer and the in-house lawyer) have been complied with that ensure the independent exercise of practice and the undisturbed observance of the rules on professional conduct and practice that apply to lawyers, see HR 24.05.2022, ECLI:NL:HR:2022:760, para 4.4.1-4.5. It must be noted that the personal scope of the national legal professional privilege is broader compared to EU law. In accordance with the case law of the Court of Justice, the legal professional privilege (in EU competition law) cannot be relied upon by in-house lawyers, see ECJ, *Akzo and Akros v Commission*, 14-09-2010, C-550/07 P. In this context, see A. de Vries and R. Widdershoven, ‘Constitutional Principles and Composite Punitive Enforcement in the EU’, pp. 48 and 51-52, in: M. Luchtman, K. Ligeti and J. Vervaele (eds), *EU Enforcement Authorities: Punitive Law Enforcement in a Composite Legal Order*, Oxford, United Kingdom, Hart, 2023.

has been accepted as a general principle of Dutch law.⁵³ It applies *mutatis mutandis* to punitive and non-punitive proceedings and is reflected by various provisions in national legislation. For the present context, it is important to emphasise that the Awb explicitly provides that ‘those who, by virtue of their office, profession or legal provision, are sworn to secrecy, may refuse to cooperate, insofar as this arises from their duty of confidentiality’.⁵⁴ In tax matters, clergymen, notaries, lawyers, doctors and pharmacists can – in derogation from the statutory rule that an obligation of confidentiality cannot be invoked to refuse cooperation with the tax authorities – refuse to comply with a demand for information by the tax authorities concerning third parties, provided that they have a professional duty of confidentiality towards those third parties.⁵⁵ The legal professional privilege cannot be invoked regarding the tax obligations of the aforementioned fiduciaries themselves. Since 2024, Dutch tax law specifies that the legal professional privilege only applies to information entrusted to fiduciaries in their professional capacity; information that becomes known to them in other capacities must be communicated to the tax authorities.

2.3.2. Right to silence and privilege against self-incrimination

The privilege against self-incrimination and the right to remain silent are crucial defence rights in Dutch administrative proceedings.⁵⁶ In their judgements, the highest administrative courts often refer to the relevant case law of the European Court of Human Rights (ECtHR). In Strasbourg doctrine, the ‘nature’ of the evidence at stake plays an important (but not decisive) role in determining whether the privilege against self-incrimination can be invoked.⁵⁷ In the wake of the ECtHR, Dutch administrative courts also distinguish between so-called ‘will-dependent evidence’ and ‘will-independent evidence’.⁵⁸ In principle, the former can trigger the application of the privilege against self-incrimination, whereas the latter cannot. Consequently, the privilege against self-incrimination primarily concerns the right to remain silent of the person who is being interrogated for the purpose

⁵³ HR 01.03.1985, ECLI:NL:HR:1985:AC9066. It must be noted that the legal professional privilege is not limited to lawyers, but also extends to notaries, doctors, pharmacists and members of the clergy. In this Chapter, we focus on the position of lawyers, but our analysis applies – *cum grano salis* – to the other fiduciaries.

⁵⁴ Article 5:20(2) Awb. See Michiels, Blomberg and Jurgens (n. 20) pp. 40 and followings.

⁵⁵ Articles 51 and 53a AWR. See M. Feteris, *Formeel belastingrecht*, Deventer, Netherlands, Kluwer, 2007, p. 281.

⁵⁶ Michiels, Blomberg and Jurgens (n. 20) p. 44.

⁵⁷ ECtHR, *Saunders v UK*, 17.12.1996, no. 19187/91. See also ECtHR, *Funke v France*, 25.02.1993, no. 10828/84; ECtHR, *J.B. v Switzerland*, 03.05.2001, no. 31827/96; ECtHR, *Chambaz v Switzerland*, 05.04.2012, no. 11663/04.

⁵⁸ Michiels, Blomberg and Jurgens (n. 20) p. 45.

of imposing a punitive sanction. They are not obligated to give a statement concerning the offence and must be cautioned on the right to remain silent before the interrogation starts.⁵⁹

In principle, documentary evidence qualifies as ‘will-independent’ material and, consequently, does not fall under the scope of the privilege against self-incrimination and the right to remain silent. Therefore, the person concerned cannot refuse to cooperate with the authorities, even if the documents and records requested contain self-incriminating information; the person concerned needs not be cautioned and can be forced to provide materials to the administrative authorities.⁶⁰ Dutch courts have recognised that documents that have been produced by the person concerned can be ‘will-dependent’.⁶¹ To that avail, the substance of the document is decisive in determining whether a statement, contained in a document, deprives a person of their right to remain silent and not to incriminate themselves of its meaning. Neither the fact that the person concerned has created the document nor the fact that their cooperation is required to obtain the documents means that the document is ‘will-dependent’.⁶²

For the specific focus of this contribution – evidence obtained from OSPs – we would argue that the right to remain silent and privilege against self-incrimination have mere marginal relevance. First and foremost, OSPs will, as a rule, not be approached to provide data concerning wrongful conduct they committed *themselves*. Instead, the information will concern other parties. Under those circumstances, the privilege against self-incrimination cannot be invoked by the OSP. Furthermore, digital evidence will often exist ‘independently of the will’, although it cannot be excluded that Dutch courts may decide that specific data qualify as ‘will-dependent’ evidence.

2.4. Legal protection against the gathering of data by Dutch administrative authorities

In the context of Dutch administrative proceedings, there shall often only be an *indirect* judicial review of the gathering of data which is relied upon as evidence to support a decision to impose an administrative fine. After an unsuccessful objection procedure before the administrative body that took the impugned sanctioning decision (*bezwaar*), it is possible to file an action

⁵⁹ Article 5:10a Awb. See Michiels, Blomberg and Jurgens (n. 20) p. 46.

⁶⁰ See CBb 04.09.2018, ECLI:NL:CBB:2018:444; CBb 07.05.2019, ECLI:NL:CBB:2019:177.

⁶¹ Michiels, Blomberg and Jurgens (n. 20) p. 45. See also De Vries (n. 17) p. 206.

⁶² See HR 21.12.2010, ECLI:NL:HR:2010:BL0666; CBb 10.04.2014, ECLI:NL:CBB:2014:116; HR 24.05.2015, ECLI:NL:HR:2015:1130; HR 24.11.2015, ECLI:NL:HR:2015:3354.

for judicial review before the competent administrative court of first instance (*beroep*).⁶³ Before Dutch tax courts, *ex post* indirect judicial review is the main rule as well.⁶⁴ The ‘affected person’ against whom the decision is issued will be able to challenge it. As a rule, this will not be the OSP from which data has been obtained, but the persons whose data was obtained; only if a decision is issued against the OSP itself will it be able to obtain an indirect judicial review by the administrative court of the measures.

It must be noted that an affected person can obtain *direct* judicial review before or during administrative proceedings through a tort action before Dutch civil courts, claiming that the administrative supervisory measures or actions amount to a wrongful act (*onrechtmatige daad*). Technically, this option is also open to an OSP, enabling it to argue that a demand for data made against it amounts to a wrongful act.

2.4.1. Legal protection before Dutch administrative (including tax) courts

In principle, access to Dutch administrative courts requires the prior existence of a ‘decision’ (*besluit*).⁶⁵ Under Dutch tax and customs law, the existence of a tax or customs decision also constitutes the central ‘entry requirement’ to obtain judicial protection before tax courts.⁶⁶ Legal action taken by an administrative body but which does not amount to a ‘decision’ can, in principle, not be subjected to direct judicial scrutiny by administrative courts.⁶⁷ A decision is ‘a written decision by an administrative body containing a legal act on the basis of public law’.⁶⁸ All criteria derived from the statutory definition of a ‘decision’ must be fulfilled before legal remedies

⁶³ Chapters 6 and 7 Awb. The judgement of the administrative court of first instance can be appealed before one of the highest courts in administrative matters: the Administrative Jurisdiction Division of the Council of State (*Afdeling bestuursrechtspraak van de Raad van State*/ABRvS), Trade and Industry Appeals Tribunal (*College van Beroep voor het bedrijfsleven*/CBB) and Central Appeals Tribunal (*Centrale Raad van Beroep*/CRvB).

⁶⁴ The judgement of the tax court in first instance can be appealed before the tax chambers of the Court of Appeals (*Gerechtshof*) and, ultimately, the Tax Division of the Supreme Court.

⁶⁵ Michiels, Blomberg and Jurgens (n. 20) pp. 51-52 and 298 and followings.

⁶⁶ Chapter V AWR and Articles 43-45 UCC. In this context, see e.g. M. Luchtman, *Grensoverschrijdende sfeercumulatie*, Nijmegen, Netherlands Wolf Legal Publishers, 2007, pp. 174-175; G. Boezelman and J. Gijsen, ‘De Algemene wet inzake rijksbelastingen’ in F. Kristen, R. Lamp, J. Lindeman, et al. (eds), *Bijzonder strafrecht*, The Hague, Netherlands, Boom juridisch, 2019, p. 263; De Vries (n. 17) pp. 214-215.

⁶⁷ Venderbos, ‘De normering van bestuurlijk toezicht- en controleonderzoek’ (n. 43) § 1.4.

⁶⁸ Article 1:3 Awb. See H. Bröring and K. de Graaf (eds), *Bestuursrecht 1. Systeem; bevoegdheid; bevoegdheidsuitoefening; handhaving*, The Hague, Netherlands, Boom juridisch, 2022, pp. 175 and followings; R. Stijnen, *Rechtsbescherming tegen bestraffing in het strafrecht en het bestuursrecht*, Deventer, Netherlands, Kluwer, 2011, pp. 231 and followings.

may be sought in accordance with administrative law. The decision to impose an administrative fine qualifies as a ‘decision’ within the meaning of the Awb.⁶⁹

The practical implementation of measures in accordance with administrative law does not amount to a decision but qualifies as ‘factual acts’ (*feitelijk handelen*). In that context, it should be specified that a written demand to cooperate with the supervisory powers of the authorities does – even if there is a risk of a sanction being imposed in case of non-compliance – not amount to a ‘decision’ in accordance with Dutch doctrine, because the resulting obligation for the person concerned follows directly from statutory law instead of the written demand.⁷⁰ It must also be observed that ‘factual supervisory acts’ can only be subjected to judicial review in so far they are relevant – e.g., if the acts have yielded useful evidence – with regard to a subsequent decision; if no decision is taken, such acts cannot be subjected to judicial review before the administrative courts.⁷¹ Due to their legal qualification, factual acts cannot be subjected to direct judicial review before administrative courts. Instead, supervisory measures that have been taken by administrative bodies based on administrative law can, as a rule, only be subjected to *indirect* judicial review by administrative courts if and in so far those measures are relevant for a subsequent decision. Thus, it is possible to challenge how data has been obtained during an objection procedure or a subsequent action for judicial review against the decision of an administrative body to impose an administrative fine, provided that the evidence has been used to prove the administrative offence and ‘support’ the fining decision.

The doctrine concerning the exclusion of unlawfully obtained evidence under Dutch administrative law provides that if the procedural rights of the person concerned are violated, and the impugned evidence is obtained as a consequence of this violation, it should be established – having regard to all circumstances of the case – whether the authorities act contrary to any general principles of proper administration, especially the principle of due care, if the evidence is used for a ‘decision’, including the decision to impose an administrative fine. The use of unlawfully obtained evidence for the purpose of tax or ‘regular’ administrative proceedings is only precluded if the

⁶⁹ Michiels, Blomberg and Jurgens (n. 20) p. 298.

⁷⁰ Ibidem, pp. 52 and 301. Since 2011, an additional instrument to obtain judicial review of information requests exists in *fiscalibus*. An ‘information decision’ (Article 52a AWR) is issued by the Tax Administration if it finds that a tax subject does not provide all required information and, therefore, does not comply with his or her obligations on the basis of the tax legislation. The tax subject can appeal the information decision. The main added value of the information decision is that the tax subject can obtain a judicial review of the lawfulness of the request before he or she is confronted with ‘negative consequences’ of non-compliance, such as a reversal of the burden of proof or punitive penalties.

⁷¹ Venderbos, ‘De normering van bestuurlijk toezicht- en controleonderzoek’ (n. 43) § 2.1.

evidence has been obtained by the authorities in a manner that is ‘manifestly improper in light of what can be expected of a properly acting public authority’ and, therefore, that the use of the evidence should be considered inadmissible in all circumstances.⁷² We refer to this criterion as the ‘manifestly improper’ criterion.⁷³

It follows from case law that the ‘manifestly improper’ criterion is assessed by the Dutch administrative courts in the light of the principle of due care and, in particular, compliance with fundamental rights.⁷⁴ Examples of violations of fundamental rights that trigger the criterion and, by extension, lead to the exclusion of evidence, are found in the context of the right to a fair trial: breaches of the right to remain silent and/or privilege against self-incrimination will lead to the exclusion of evidence.⁷⁵ Dutch administrative courts have also recognised that violations of the principle of non-discrimination are ‘manifestly improper’ and require the exclusion of the impugned evidence.⁷⁶ For the present contribution and its focus on the role of OSPs, however, it is most important that violations of the right to private life may warrant the exclusion of evidence. In this regard, illustrations can be found in cases that concern the use of (intrusive) digital techniques or technologies to gather evidence in administrative proceedings without an explicit or specific legal basis, but it can also be derived from Dutch case law

⁷² HR 01.12.1992, ECLI:NL:HR:1992:ZC5028, r.o. 3.2.5.

⁷³ A. Duijkersloot, A. de Vries and R. Widdershoven, ‘The Netherlands’ in F. Giuffrida and K. Ligeti (eds), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, Luxembourg, University of Luxembourg, 2019, pp. 197-215. For Dutch literature on the ‘manifestly improper’ criterion, see e.g. YE Schuurmans, ‘Onrechtmatig verkregen bewijsmateriaal in het bestuursrecht’ *AA*, 2017, pp. 389-390; Michiels, Blomberg and Jurgens (n. 20) p. 410.

⁷⁴ Duijkersloot, De Vries and Widdershoven (n. 73) pp. 203-204; Schuurmans, ‘Onrechtmatig verkregen bewijsmateriaal in het bestuursrecht’ (n. 73) pp. 392-393; Venderbos, ‘De normering van bestuurlijk toezicht- en controleonderzoek’ (n. 43) § 2.2.

⁷⁵ See HR 12.03.1997, ECLI:NL:HR:1997:ZC6589; 20.03.2015, ECLI:NL:HR:2015:643, para 2.5.2. See also Duijkersloot, De Vries and Widdershoven (n. 73) pp. 203-204. If an administrative authority hears a person with the purpose of imposing an administrative fine but does not provide the person concerned the required caution on the right to remain silent, the statement will be excluded, see e.g. ABRvS 27.06.2018, ECLI:NL:RVS:2018:2115; CBb 06.04.2021, ECLI:NL:CBb:2021:366; Opinion AG Keus 12.04.2017, ECLI:NL:RVS:2017:1034. Similarly, self-incriminating statements that have been obtained while the person concerned was held to cooperate with the authorities during monitoring shall be excluded from punitive administrative proceedings. In our view, the use of will-dependent evidence that is subject to a restriction on use is ‘manifestly improper’ as well, see also R. Widdershoven, H. Addink, J. Bootsma, et al. (eds), *Europa en het algemeen bestuursrecht. Burger en bestuur in de gemeenschappelijke rechtsorde*, The Hague, Netherlands, Boom juridisch, 2021, p. 172; De Vries (n. 17) p. 268.

⁷⁶ Schuurmans, ‘Onrechtmatig verkregen bewijsmateriaal in het bestuursrecht’ (n. 73) pp. 393-394. See ABRvS 03.06.2015, ECLI:NL:RVS:2015:1723; CRvB 14.04.2015, ECLI:NL:CRVB:2015:1228.

that demands for information from third parties – eg, OSPs – may be disproportionate and, therefore, could render the subsequent use of the data ‘manifestly improper’.⁷⁷ In the latter context, much depends on the facts and circumstances of the case, including the character and amount of required data and the available alternatives to get the data.

2.4.2. Legal protection before Dutch civil courts

As a rule, it is not possible to challenge supervisory measures before the competent Dutch administrative or tax courts prior to the appeal against a ‘decision’. The resulting ‘gap’ in legal protection is filled by the option to launch a procedure before a civil court.⁷⁸ In short, Dutch civil courts function as a ‘safety net’ if no legal remedies exist before the ‘specialised’ (administrative or criminal) courts. With regard to the gathering of data as evidence, judicial protection by Dutch civil courts is triggered through the start of a tort action: the affected party should claim that an administrative authority is acting in a wrongful manner through the order or implementation of a supervisory measure.⁷⁹ The plaintiff – which could be an OSP – can request the court to prohibit the administrative authority from taking the impugned action. As part of their review, civil courts are competent to scrutinise the actions of public authorities in accordance with public law. For judicial protection by civil courts to be ‘effective’, it shall often be required to launch civil interim relief proceedings. When it is argued that fundamental rights are at stake or have been violated due to the (intended) measures of the administrative authorities, civil courts will perform a stringent review, also in the context of interim relief proceedings.⁸⁰

Regarding the gathering of data by administrative authorities, there are several examples of civil interim relief proceedings against, *inter alia*, the

⁷⁷ For the disproportionality of a demand for information CRvB 11.10.2018, ECLI:NL:CRVB:2018:3205, r.o. 4.4.3. For example, the use by administrative authorities of (long-term) audio-visual recordings of someone’s dwelling or workspace or systematic GPS-tracking through means of a technical device – measures for which no specific legal basis exists under Dutch administrative law – constitutes serious infringements of Article 8 ECHR and, by extension, makes the use of the collected evidence ‘manifestly improper’ (see also Section 3.3.2). See CRvB 13.09.2016, ECLI:NL:CRVB:2016:3479; CRvB 15.03.2016, ECLI:NL:CRVB:2016:947; CRvB 20.12.2022, ECLI:NL:CRVB:2022:2792. See also Crijns and Van Emmerik (n. 42) pp. 241 and followings; Venderbos, ‘De normering van bestuurlijk toezicht- en controleonderzoek’ (n. 43) § 3.1.1; Schuurmans, ‘Onrechtmatig verkregen bewijsmateriaal in het bestuursrecht’ (n. 73) pp. 396-397.

⁷⁸ Michiels, Blomberg and Jurgens (n. 20) p. 301; F. Michiels and R. Widdershoven, ‘Handhaving en rechtsbescherming’ in F. Michiels and E. Muller (n. 21) p. 97; Stijnen (n. 68) p. 232. See also De Vries (n. 17) p. 215.

⁷⁹ See H. Tolsma and A. Marseille (eds), *Bestuursrecht 2. Rechtsbescherming tegen de overheid*, The Hague, Netherlands, Boom juridisch, 2022, p. 395 and followings.

⁸⁰ In this context, see eg Rb. Den Haag 12.07.2017, ECLI:NL:RBDHA:2017:7968, para 4.5.

demand to surrender information to the authorities, and the inspection of electronic information and its copying.⁸¹ These proceedings are sometimes started *before* the plaintiff has given effect to a demand or has been subjected to a measure, because the plaintiff finds that the demand or measure is unlawful or disproportionate. It follows from case law that interim relief proceedings are also launched to challenge the relevance or character of the information data that has been inspected and/or copied by the administrative authorities. Examples include proceedings concerning the inclusion of private data or privileged information in the information that was obtained by the authorities. The proceedings do not seem to be ‘successful’ as the factual actions of the administrative authorities and the available safeguards in selected policy areas are considered to meet the required standards according to Dutch civil courts. None of the aforementioned proceedings were started by OSPs to challenge the demand for data made against it.

3. PUNITIVE ADMINISTRATIVE PROCEEDINGS: SECTORIAL FRAMEWORK

In this Section, we provide an overview of the applicable sectorial frameworks. When the sectorial frameworks do provide specific rules and procedures, regard should be had to the general framework (see Sections 2 and 4).

3.1. Requests for data to online service providers

As mentioned before, the Awb provides a general framework for administrative proceedings, including supervisory powers to gather data as evidence (see Section 2.2.1). Sectorial legislation may provide additional procedural rules. Tax and customs proceedings are not governed by the general rules of administrative procedure as derived from the Awb.

3.1.1. Customs and tax (VAT) enforcement

Tax proceedings, including VAT procedures, follow the rules from the AWR, whereas customs proceedings are governed by the ADW and, in EU customs matters, the UCC.

In accordance with Dutch tax law, each person is held to provide at the request of the tax authorities the data and information which may be relevant for their taxation, and to make available for this purpose the books, records and other data carriers or the contents thereof – at the discretion of the

⁸¹ See District Court Den Haag 12.07.2017, ECLI:NL:RBDHA:2017:7968; District Court Den Haag 22.11.2017, ECLI:NL:RBDHA:2017:14150; District Court Den Haag 10.10.2018, ECLI:NL:RBDHA:2018:12722; Court of Appeal Den Haag 12.02.2019, ECLI:NL:GHDHA:2019:470.

authorities – the inspection of which may be of importance for the determination of the facts that may influence the taxation.⁸² ‘Books, records and other data carriers’ should be interpreted in a broad manner: all information carriers, including digital information carriers, are covered, for instance (digital) accounts, (digital) draft accounts, till rolls, notes and receipts, deeds, letters, emails, minutes, computer files, CD-ROMs, videos, diaries, orders, quotations, contracts, microfilms, shipping lists, and order confirmations.⁸³ Information and books, records and other data carriers of the tax subject can also be required if they are (temporarily) held by a third party.⁸⁴ The authorities can make copies of the data and information.⁸⁵ To perform a tax inspection, the authorities are able to enter premises or plots of land; they should be given access if required.

Under customs law, the authorities are competent to inspect documents and question persons. Customs officials can request information from any person directly or indirectly involved in the accomplishment of customs formalities or in customs controls, including third parties, and make copies of the relevant information carriers or their content.⁸⁶ Customs authorities are allowed to enter premises; dwellings can only be entered with the ‘informed consent’ of the occupant or with prior authorisation of the Inspector.⁸⁷

Demands for digital information in Dutch tax and customs proceedings can be made against private actors. Such demands can, first and foremost, be made against the tax or customs subject, but also against third parties.⁸⁸ In tax proceedings, a demand against a third party can only be made if that party is required to keep an administration.⁸⁹ This means that banks, accounting firms and, presumably, OSPs that are located in the Netherlands can be required to communicate information to the tax authorities, provided that it is compatible with general principles of good administration.⁹⁰ Under customs law, a similar provision is found.⁹¹ Third parties include accounting firms, customs expeditors or transporters, but also airlines, banks and, presumably, OSPs.⁹²

⁸² Article 47(1) AWR. Feteris (n. 55) pp. 274-275; Boezelman and Gijzen (n. 66) p. 259.

⁸³ Feteris (n. 55) p. 275; L. Wijsman, *Nemo tenetur in belastingzaken*, Deventer, Netherlands, Kluwer, 2017, p. 237. See also *Kamerstukken II* 1988/89, 21287, No 3, 5 and 23.

⁸⁴ Article 48 AWR.

⁸⁵ Article 49 AWR.

⁸⁶ Douane, *Handboek Douane*, Rotterdam, Netherlands, Douane, 2016 edn, 2016, Section 10.2.3. The broad interpretations concerning ‘books, records and other data carriers’ also applies vis-à-vis the ‘documents’ that can be demanded in customs matters.

⁸⁷ Article 1:23(4) ADW.

⁸⁸ Boezelman and Gijzen (n. 66) p. 260; Douane (n. 82) Section 10.2.1.

⁸⁹ Article 52 AWR.

⁹⁰ Feteris (n. 55) pp. 279-280.

⁹¹ Article 1:32 ADW.

⁹² Douane (n. 82) Section 10.2.1. In this context, see also *Kamerstukken II* 2006/07, 30 580, No 3, 108.

Unlike other Dutch administrative authorities, the Douane and Belastingdienst do not have a specific practice for gathering data as evidence. To be more precise, we have neither been able to find information on such practice that is available to the general public, nor have we been able to establish the existence of internal rules or guidelines used by the authorities. Of course, the statutory rules on the observance of the legal professional privilege and the limitations regarding using private information (general principles of good administration and Article 8 ECHR) provide a general framework that must be observed when data as evidence is concerned.

Although Dutch tax and customs authorities can make demands for information to OSPs, it seems that this is quite rare and, if such demands are made, they remain limited in scope. In our view, this must be understood against the background of the main characteristics of the Dutch enforcement architecture, specifically in tax and customs matters. First and foremost, intrusive and/or covert investigative measures are reserved for criminal proceedings *sensu stricto*, meaning that such measures cannot be relied upon for the purpose of, *inter alia*, tax supervision or the imposition of administrative fines. Demands for information to OSPs may relate to data – for instance, traffic and location data – that would enable the authorities to obtain a detailed picture of (aspects of) the private life of the person concerned. Such demands constitute a serious interference with the right to private life and are, in accordance with Dutch doctrine, reserved for criminal investigations. Secondly, the enforcement task of the tax and customs authorities is primarily to establish and/or verify the correct tax debt (fiscal supervision). Thus, their enforcement efforts are also focused on that task. While the Dutch tax and customs authorities can also conduct investigations into breaches of the applicable fiscal legislation and impose, if appropriate, an administrative fine or a so-called ‘fiscal penalty order’ their investigative and ‘punitive’ competences are, in practice, reserved to minor and uncomplicated cases that do not require (much) additional investigation.⁹³ This means that tax and customs authorities will, in principle, not demand data from an OSP for ‘investigative’ purposes. Instead, serious or complex cases will be reported to the OM and shall be investigated by the FIOD.

⁹³ In this context, see De Vries (n. 17) pp. 160-162. Although reports concerning fiscal offences should, in derogation of the main rule under Dutch law, be communicated to the Douane and Belastingdienst instead of the OM, serious cases (including cases that require the application of coercive measures, including pre-trial detention) must be forwarded to the OM.

3.1.2. Punitive enforcement in the area of banking law and financial markets

The AFM and/or its officials have several administrative powers that allow the gathering of data. Some of these powers are available on the basis of the Awb and follow its general procedural norms, but the Wft also provides some specific rules. In accordance with the Wft, for example, the AFM itself – instead of its officials – is competent to demand information from anyone to perform its statutory market surveillance duties.⁹⁴ The AFM is only awarded the power to demand information; the power to inspect documents and records and to make copies is not mentioned. Compared to the general framework under the Awb, this constitutes a significant and potentially impactful gap in the available administrative powers of the AFM, but it has been recognised in Dutch case law that consistent interpretation with EU law implies that the power to demand information *also* covers the power to make copies of the information obtained.⁹⁵

The power to demand information and the power to inspect business documents and records can be applied to anyone. This means the powers can also be relied upon *vis-à-vis* third parties, including OSPs.⁹⁶ The supervisor must adhere to the principles of proportionality and subsidiarity, and should guarantee observance of the legal professional privilege. The principles of proportionality and subsidiarity can preclude that supervisory powers are relied upon against third parties, especially if those third parties are not themselves involved in activities to which the Wft applies.⁹⁷

The gathering of data by the AFM can raise questions concerning the private and/or privileged nature of the data. The so-called Working Method AFM inspection and copying of data (*Werkwijze AFM inzien en kopiëren van digitale gegevens 2020*, *Werkwijze AFM 2020*) provides detailed rules concerning the inspection and copying of digital data during administrative investigations.⁹⁸ In short, the *Werkwijze AFM 2020* – which constitutes a so-called binding regulation of an independent administrative authority (*regeling zbo*) – sets out step-by-step how private and/or privileged data should be ‘cleaned’ from the initial data set obtained during an administrative investigation. Often, the data will be obtained from the person concerned, but it can also be obtained from a third party, such as an OSP. In the latter case, it

⁹⁴ Article 1:74 Wft.

⁹⁵ CBb 21.09.2015, ECLI:NL:CBB:2015:288.

⁹⁶ M. van Eersel, *Handhaving in de financiële sector*, Deventer, Netherlands, Kluwer, 2022, pp. 33-34.

⁹⁷ *Ibidem*, p. 33.

⁹⁸ *Werkwijze AFM inzien en kopiëren van digitale gegevens [2020] Stcrt.* 13499. See also Van Eersel (n. 96) p. 38; Roth and Hillen, ‘Digitaal onderzoek door de AFM. Hoe gaat dat in zijn werk, mag dat zomaar en hoe adequaat is de rechtsbescherming’ (n. 44) pp. 774-775.

will be the persons whose data is concerned that can raise questions about the private and/or privileged nature of the data, provided that they know the data has been obtained.

The investigator – an official of the AFM who is a ‘supervisor’ within the meaning of the Awb – decides, in light of the aim of the investigation, which digital data shall be required from the subject of the investigation. Subsequently, the so-called IT specialist – a designated official of the AFM who is not involved in the substantive investigation – ensures that this data is identified, secured and copied. The data is transferred to the AFM office and saved there. At this point, the supervisor has no access to the data. Within five working days of copying the data, the IT specialist will provide an overview of the copied data to the subject of the investigation and informs the subject of the option to ‘clean’ the data of personal and/or privileged data. A reasoned request to clean the data should be filed within ten working days. If a request is not made within this period or if the subject of the investigation states that it shall not make a request to clean the data, the IT specialist will provide the supervisor access to the data after written confirmation to the subject of the investigation.⁹⁹ If a request to clean the data is filed, the IT specialist will assess the claimed private and/or privileged data in light of the reasons put forward in the request. In principle, cleaning of the data will take place at the office of the AFM in the presence of (legal representatives of) the subject of the investigation. If the subject of the investigation can indicate unequivocally and with precision which data is private or privileged, the cleaning of data will be performed at the office of the subject, unless there are technical or other practical obstacles.¹⁰⁰

If the IT specialist finds that the claim concerning the privileged nature of data is, in whole or in part, unfounded, the subject of the investigation can, within ten working days of the notification, require an assessment of the data by the so-called Confidentiality Officer. The involvement of the Confidentiality Officer can also be invoked if the subject of the investigation argues that a cursory look at the data by the IT specialist compromises the privileged nature of the data.¹⁰¹ If the Confidentiality Officer finds that (part of) the claim concerning the privileged nature of the data is justified, they require that the IT specialist cleans the data from the file; the data will be destroyed. If the Confidentiality Officer finds that (part of) the claim is not justified they will inform the subject of the investigation. In that case, the data will not be made available to the supervisor for a period

⁹⁹ Article 2 Werkwijze AFM 2020.

¹⁰⁰ Article 3 Werkwijze AFM 2020.

¹⁰¹ Articles 3 and 4 Werkwijze AFM 2020.

of ten working days to allow the subject to launch civil interim relief proceedings to challenge the outcome of the assessment.¹⁰²

After the data is cleaned, the IT specialist enables the supervisor to access it. The supervisor exclusively performs targeted actions in the cleaned data through searching terms, unless the purpose of the investigation means that the data as a whole is relevant. If private and/or privileged data is discovered during the actions of the supervisor this data will be cleaned. Relevant digital data will be added to the case file. All other data will be destroyed.¹⁰³

3.1.3. Competition law enforcement

The ACM holds several administrative powers which allow its officials to gather data. While most of these powers are available based on the Awb, EU law provides an additional legal basis for the ACM to carry out inspections or other fact-finding measures on behalf and for the account of the competition authority of another Member State to establish whether there has been an infringement of Article 101 or 102 of the TFEU.¹⁰⁴ Additionally, the ACM shall undertake the inspections which the Commission considers to be necessary or which it has ordered.¹⁰⁵ ACM officials shall conduct these inspections in accordance with national law and, therefore, where digital information needs to be inspected, the ACM shall do so based on the Awb, particularly on the basis of Article 5:17 Awb which allows its officials to inspect business information and documents.¹⁰⁶ While Article 6b of the ACM Establishing Act seems to copy this provision, the ACM relies on the Awb when engaging in punitive enforcement action.¹⁰⁷ Only where the ACM exercises its monitoring and exploratory investigative powers, the Establishing Act functions as a general legal basis. However, in the context of the obligation for private actors to cooperate fully with the supervisory authority, the ACM relies on the Establishing Act in the context of punitive enforcement procedures too.¹⁰⁸

In 2014 the ACM published a document in which it explains its working method with regard to the ACM's power to demand access to digital

¹⁰² Article 4(4) Werkwijze AFM 2020.

¹⁰³ Articles 5 and 6 Werkwijze AFM 2020.

¹⁰⁴ Article 22(1) of the Council Regulation 1/2003. See also Article 24(2) of the Directive (EU) 2019/1 ECM.

¹⁰⁵ Council Regulation 1/2003, Article 22(2).

¹⁰⁶ See preamble of the ACM Werkwijze voor onderzoek in digitale gegevens 2014; ACM Interview 08.02.2024.

¹⁰⁷ See ACM Establishing Act, Article 6B.

¹⁰⁸ ACM Interview 08.02.2024.

information on the basis of Article 5:17 Awb.¹⁰⁹ This working method prescribes which persons may be subject to information requests and the procedures according to which it is determined which digital information shall form part of the investigative file.

The working method prescribes that digital information can be requested by the ACM as long as this is reasonably required for the performance of the supervisory authority's tasks.¹¹⁰ Requests can include both content and metadata, as long as it relates to business information. This means that a large variety of data – such as email data, mailboxes, chat applications, files – can be examined at, for example, telephones, computers or notebooks.¹¹¹ Metadata is considered relevant, especially when the ACM requires information about the edits made to the digital information (e.g., when, where and by whom).¹¹² According to the ACM's working method, the persons to whom information requests are directed are so-called 'targets' of the ACM.¹¹³ Such targets can be anyone in accordance with the Awb and, therefore, may include OSPs as well. Targets are carefully selected based on an internal working method of the ACM, but it differs per investigation which persons are a target to the ACM, i.e., it is not necessarily always the director of a supervised entity.¹¹⁴ A natural person can only form a target when there is a suspicion of the person's involvement in the purpose and object of the investigation.¹¹⁵ Before exercising its powers in accordance with Article 5:17 Awb, the ACM needs to inform the persons whose information is sought the reason as to why a supervisory power is exercised, which functions as a safeguard to fishing expeditions. The working method does not determine whether this shall be done verbally or in (digital) writing.¹¹⁶

The inspection of data held by third parties, such as OSPs, usually takes place only after an explicit request from the ACM, and not by means of the voluntary sharing of information by the third party. After all, the voluntary sharing of information by an OSP may lead to a contractual breach with the supervised entity or person concerned, and/or a violation of the EU's data protection standards.¹¹⁷ Voluntary sharing of data by persons connected to the supervised entity, only happens in the context of leniency requests, which

¹⁰⁹ ACM Werkwijze voor onderzoek in digitale gegevens 2014, p. 6.

¹¹⁰ Article 5:13 Awb.

¹¹¹ ACM Interview 08.02.2024

¹¹² ACM Interview 08.02.2024.

¹¹³ Article 5:13 Awb; ACM Interview 08.02.2024.

¹¹⁴ Concerning the preparation of company visits (*bedrijfsbezoeken*).

¹¹⁵ Article 2.1(2) ACM Werkwijze voor onderzoek in digitale gegevens 2014.

¹¹⁶ Article 2.1(3) ACM Werkwijze voor onderzoek in digitale gegevens 2014.

¹¹⁷ ACM Interview 08.02.2024.

may lead to a settlement of the case instead of the imposition of penalties.¹¹⁸ Where the ACM requests access to data held by an OSP, the latter is obliged to cooperate with the ACM.¹¹⁹ While the refusal or failure of *the infringer* to comply with demands by the ACM may lead to the imposition of an administrative penalty of a maximum € 900.000 or 1% of the entity's revenue if this amount is higher in accordance with Article 12m of the ACM's establishing act, such an administrative penalty cannot be imposed on third parties violating Article 5:20 Awb.¹²⁰ Furthermore, a violation of Article 5:20(1) Awb does not constitute a criminal offence in accordance with Article 184 WvSr. The ACM officials, however, argue that this is not a problem in daily practice since third parties usually cooperate with the supervisory authority.¹²¹

Importantly, if data is will-dependent, the target can refuse to cooperate with the authorities where the requested documents contain self-incriminating information. According to the ACM, digital information becomes will-dependent where the ACM would request the editing of information or the provision of information in a particular form or format.¹²² Furthermore, the target needs to be cautioned and cannot be forced to provide will-dependent materials to the administrative authorities if the information is gathered with a view to imposing a punitive sanction.¹²³ The caution is generally granted when the ACM demands access to digital information on-site, even when the ACM does not yet know whether a punitive sanction will be imposed.¹²⁴ All concerned employees of the undertaking under investigation are cautioned.¹²⁵ This guarantees that will-dependent information can be used, also when the ACM decides at a later stage to commence punitive enforcement action.¹²⁶

When inspecting the requested business documents and records, the supervisor can also make copies.¹²⁷ To that avail, the supervisor can take the documents and records briefly, by storing the information in an encrypted dataset (*veiliggestelde dataset or secured dataset*) in an IT environment called

¹¹⁸ ACM Interview 08.02.2024. See also ACM Richtsnoeren vereenvoudigde afdoening van boetezaken.

¹¹⁹ Article 5:20 Awb; ACM Interview 08.02.2024.

¹²⁰ Article 12m(1) ACM Establishing Act.

¹²¹ Nevertheless, if needed Article 5:15(2) Awb could potentially function as a means to access a dwelling of a third party that refuses to cooperate, with the help of the police. See also Article 12b(2) of the ACM Establishing Act which prescribes that ACM officials may exercise their powers under Article 5:17 Awb in accordance with Article 5:15(2) Awb.

¹²² ACM interview 8.2.2024.

¹²³ See Article 5:10a Awb and Article 12i ACM Establishing Act.

¹²⁴ See Article 5:10a Awb and Article 12i ACM Establishing Act; ACM Interview 08.02.2024.

¹²⁵ Article 12i ACM Establishing Act.

¹²⁶ ACM Interview 08.02.2024.

¹²⁷ Article 5:15(2) Awb.

Cryptshare.¹²⁸ A hashcode shall be connected to the data to make sure that the data cannot be edited, wherefore IT specialists always accompany and assist ACM officials.¹²⁹ This encrypted dataset shall not entail personal documents and business documents covered by legal professional privilege, since these documents cannot be inspected and/or copied. Therefore, where data is accessed on-site, officials will quickly scan the materials for business and privileged information in order to prevent the collection of non-business related and privileged materials.¹³⁰ However, when looking at the size of collected datasets, it is not unlikely that these nevertheless entail personal or privileged data.¹³¹ The Awb does not prescribe how administrative authorities should guarantee that personal documents or documents covered by legal professional privilege should be ‘filtered’ from the materials obtained by the administrative authorities. In that regard, the ACM’s working method regarding the power to demand access to digital data does prescribe that once all data is collected and stored in the secured dataset, this dataset shall be analyzed in order to determine which information entails privileged, or non-business related information.¹³² This information shall be deleted from the dataset before it qualifies as a so-called ‘within-the-scope’ dataset (*binnen de reikwijdte dataset*).¹³³ A within-the-scope dataset only entails data that, by its nature and/or content, can reasonably fall within the purpose and object of the investigation.¹³⁴ The ACM’s working method on digital information does not determine who exactly is responsible for analysing the secured dataset regarding non-business-related information. However, according to the ACM officials, it is not the investigation team itself who shall conduct this analysis, since it has no access to the secured dataset – nor does the investigation team have access to the within-the-scope dataset.¹³⁵

The working method on the inspection of digital information, furthermore, prescribes that persons concerned are allowed to be present when the ACM determines which information falls within the scope of the purpose and object of the investigation.¹³⁶ Furthermore, these persons concerned shall receive an overview of the data that is included in the ‘within-

¹²⁸ In order to comply with the EU’s General Data Protection Regulation 2016/679.

¹²⁹ Article 2.1(5) and p. 8 ACM Werkwijze voor onderzoek in digitale gegevens 2014. A hashcode will protect the ‘integrity of the digital file’.

¹³⁰ ACM Interview 08.02.2024; Article 3 ACM Werkwijze geheimhoudingsplicht advocaat 2014.

¹³¹ ACM Interview 08.02.2024.

¹³² Article 1(4) ACM Werkwijze voor onderzoek in digitale gegevens 2014.

¹³³ Article 1(5) ACM Werkwijze voor onderzoek in digitale gegevens 2014.

¹³⁴ Article 1(4) ACM Werkwijze voor onderzoek in digitale gegevens 2014.

¹³⁵ ACM interview 8.2.2024.

¹³⁶ Article 2.2(2) ACM Werkwijze voor onderzoek in digitale gegevens 2014.

the-scope' dataset and the way this data was selected.¹³⁷ Before the within-the-scope dataset is turned into the 'investigate dataset' (*onderzoeksdataset*), the persons concerned shall have the possibility to request the deletion of further non-business-related information. The person concerned shall have to do so in writing and provide reasons for their claim.¹³⁸ However, the ACM shall only allow for this possibility if it can reasonably be expected that the within-the-scope dataset entails further non-business-related information.¹³⁹ In other words, the right to claim non-business-related information is not absolute.

Interestingly, the working method defines persons concerned as the addressees of the ACM's exercise of competences related to Article 5:17 Awb.¹⁴⁰ This seems to imply that where a third party, such as an OSP, is the addressee of an information request, this third party shall qualify as an concerned party, meaning that this third party shall have access to the within-the-scope dataset in order to assess it on non-business-related and privileged information. This, however, does not seem to align with the actual purpose of such a right and the actual working practice of the ACM according to which a third party is never granted access to any dataset or the file.¹⁴¹

After the person concerned has had access to the within-the-scope dataset to claim non-business-related or privileged information if necessary, the within-the-scope dataset shall be turned into a so-called 'investigative dataset' which shall form part of the investigative file and which is accessible to the investigation team.

According to the obligation of legal professional privilege, all information exchanged between the lawyer and their client in their respective capacities is protected, and the lawyer cannot be required to communicate this information to the authorities verbally or in writing. Therefore, the ACM is not allowed to consult documents or files which comprise information that falls under the legal professional privilege. As discussed previously, the ACM shall delete all information exchanged between the lawyer and their client from the secured dataset. The ACM officials confirm that this is done by IT experts, meaning that the investigation team will never have access to this information.¹⁴² After the person concerned has had the opportunity to access the 'within-the-scope dataset' and it wishes to have further privileged data removed, this request shall be examined by the legal professional privilege

¹³⁷ Article 2.2(3) ACM Werkwijze voor onderzoek in digitale gegevens 2014.

¹³⁸ Article 2.3(1) ACM Werkwijze voor onderzoek in digitale gegevens 2014.

¹³⁹ Persons concerned shall also have to possibility to request the deletion of further privileged information, see Section 3.2.2.

¹⁴⁰ Article 1(3) ACM Werkwijze voor onderzoek in digitale gegevens 2014.

¹⁴¹ ACM Interview 08.02.2024.

¹⁴² ACM Interview 08.02.2024.

officer (*functionaris verschoningsrecht*).¹⁴³ When the claim is accepted, the legal professional privilege data is removed from the within-the-scope dataset.¹⁴⁴ Only then the dataset will be considered ready to be shared with the investigation team. In cases where privileged data has nevertheless been missed and was, therefore, not removed before the dataset was shared with the investigation team, this privileged data shall be set aside once discovered.¹⁴⁵

3.1.4. GDPR enforcement

The AP relies both on the Awb and the GDPR when exercising its powers in supervising and enforcing the GDPR, for which it holds powers to gather data.¹⁴⁶ First, Article 58(1) of the GDPR lays down harmonised investigative powers for all data protection authorities established within the EU. Based on this provision, the AP is empowered to order the controller and the processor to provide any information it requires for the performance of its tasks,¹⁴⁷ to obtain from the controller and the processor access to all personal data and all information necessary for the performance of its tasks,¹⁴⁸ and to obtain access to any premises of the controller and the processor, which includes access to any data processing equipment and means.¹⁴⁹ Additionally, the GDPR provides a legal basis for the AP to carry out inspections and investigations on request of a DPA of another Member State,¹⁵⁰ or to carry out joint inspections and investigations.¹⁵¹ Hence, the GDPR provides the AP a broad legal basis to order the provision of or access to any information, including digital information. When exercising its investigative powers, the AP does not solely rely on the GDPR, but instead, also on the Dutch Awb.¹⁵² Reliance on the Awb is particularly important where information is requested from actors other than the controller and processor since the Awb entitles the AP to request digital information from *anyone*, while the GDPR only allows for the requesting of information from the *controller* and *processor*.¹⁵³ Hence, on the basis of the Awb, the AP is able to request information from OSPs,

¹⁴³ ACM Werkwijze geheimhoudingsprivilege advocaat 2014, Articles 2 and 5.1.

¹⁴⁴ ACM Werkwijze geheimhoudingsprivilege advocaat 2014, Article 5.2.

¹⁴⁵ ACM Interview 08.02.2024.

¹⁴⁶ Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data.

¹⁴⁷ Article 58(1)(a) GDPR.

¹⁴⁸ Article 58(1)(e) GDPR.

¹⁴⁹ Article 58(1)(f) GDPR.

¹⁵⁰ Article 61(1) GDPR.

¹⁵¹ Article 62(1) GDPR.

¹⁵² Articles 5:16 and 5:17 Awb; AP Interview 05.03.2024.

¹⁵³ AP Interview 05.03.2024.

which it would not be able to do under the GDPR only. Furthermore, Article 5:15 Awb may function indirectly as a legal basis to gather digital information, since it empowers the AP to enter a place to conduct on-site inspections and demand the inspection of business documents as part of the on-site inspection. The AP officials argue that it cannot, based on this provision, enter *digital* places – e.g., by breaking through an encryption of electronic equipment.¹⁵⁴ Instead, the AP generally demands cooperation from the party under investigation to access digital information. Article 58(1)(f) of the GDPR, however, seems to empower the AP to enter also digital places, as this provision offers a legal basis to the AP to obtain access to any premises of the controller or data processor, which includes access to data processing equipment and means.

While the GDPR – and the Awb implicitly – entitle the AP to request and collect digital information, detailed practices are not established by these laws, nor by working methods of the AP itself. Therefore, the AP relies on the ACM's working method regarding the ACM's power to demand access to digital information.¹⁵⁵ This working method prescribes which persons may be subject to information requests and the procedures according to which it is determined with digital information shall form part of the investigative file (see Section 3.1.4). An important difference, however, as regards the inspection of data contains the type of data that is being inspected. While the AP can, just like the ACM, inspect a large variety of data – both meta and content data – the AP often relies on telemetry data as a starting point for collecting relevant information too. Telemetry data offers the AP insights into the transmission of personal data to other (remote or invisible) devices.¹⁵⁶ Such telemetry data then reveals, for example, to which other computers personal data is being transmitted, which can reveal large and complex networks in which personal data is being shared. Such telemetry data could even reveal that a third party, like an OSP, working with the controller under investigation bears responsibility for the processing activity too.¹⁵⁷ It may then turn out that not one controller, but multiple controllers or both the controller and the processor are responsible for the processing activity, and shall therefore also qualify as a party under investigation to whom enforcement measures may be addressed.¹⁵⁸ In this regard, it is highly important for the AP to clearly determine the scope of the investigation,

¹⁵⁴ AP Interview 05.03.2024.

¹⁵⁵ ACM Werkwijze voor onderzoek in digitale gegevens 2014, p. 6. Note that the AP is at the time of the interview working on its own working method, in which it is being assisted by the ACM.

¹⁵⁶ AP Interview 05.03.2024.

¹⁵⁷ See for a definition of a controller, processor and joint controller, Articles 4(7)(8) and 26 GDPR.

¹⁵⁸ AP Interview 05.03.2024.

before commencing it, which is also being communicated to the party under investigation.¹⁵⁹ If the investigation of the alleged violation sheds light on a suspicious role of other parties and/or additional violations of the GDPR, the AP aims to stick to this well-defined scope of the initial investigation, while investigating the additional infringements via a separate enforcement procedure.¹⁶⁰ This helps to prevent that other actors become parties under investigation as well. While the distinction of third party or (joint) controller/processor does not have consequences for the exercising of the AP's investigative powers, it would have consequences for the imposition of enforcement measures and the safeguarding of procedural rights where third parties become parties under investigation too – e.g., third parties cannot rely on the privilege against self-incrimination and the right to remain silent,¹⁶¹ while this is different where it turns out that a third party can be qualified as a (joint)controller or processor subject of the investigation too.

As established by the Awb, since anyone is held to provide all cooperation with the supervisor, that can reasonably be demanded, this obligation extends also to third parties, such as OSPs.¹⁶² While the refusal or failure of this actor to comply with the demands of the AP generally leads to the imposition by the AP of an administrative penalty payment, implying that the actor should pay an amount of money if the demand is not (timely) complied with, the refusal also constitutes a criminal offence. In practice, this offence is hardly ever prosecuted. The GDPR adds to this that where a *controller* or *processor*, and where applicable their representatives, do not comply with the AP's demands, this may lead to the imposition of an administrative fine of a maximum € 10.000.000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.¹⁶³ This fine can, therefore, not be imposed on OSPs who deny cooperation with the AP.

Where data is will-dependent, cooperation with the AP can be refused where the requested documents contain self-incriminating information. Similar to the ACM, the AP often sees the existence of data independent of the will of the person concerned. However, data becomes will-dependent if it requires, for example, the editing of information. Questions posed or explanations asked regarding data also form will-dependent

¹⁵⁹ This is not required by the Awb, UAVG of the GDPR, but is nevertheless a well-established working method of the AP. Therefore, prior to commencing the investigation, the AP communicates both the data processing activity subject to the investigation, and the suspected infringement to the controller or processor.

¹⁶⁰ AP Interview 05.03.2024.

¹⁶¹ ACM Interview 08.02.2024.

¹⁶² Article 16 UAVG, in conjunction with Article 5:32(1) Awb.

¹⁶³ See Articles 31 and 83(4)(a) GDPR.

information. On the other hand, actions that are required to access digital information are not seen as will-dependent. Hence, the use of a password, fingerprint or iris scan are will-independent actions.¹⁶⁴ Where information is will-dependent and may contain self-incriminating information, the party needs to be cautioned. While some departments do this in an early stage of the investigation to prevent the situation that the information gathered cannot be used for possible further punitive enforcement action, other officials do this only when they clearly foresee the imposition of an administrative fine.¹⁶⁵ The caution is generally granted only to the director or representative of the controller or processor, but not to any other staff member. Where information is requested via mail or email, the AP includes an anticipative clause in its text, stating that the party is obliged to provide the requested documents (if available) while they are not obliged to answer questions.

4. TRANSFER OF DATA BETWEEN PROCEEDINGS

Under Dutch law, there are no specific rules on the processing of information obtained from third parties, notably OSPs. Instead, general and sectorial rules and doctrine dictate the transfer of data between (administrative and judicial, domestic and foreign) authorities, and the eventual use of the evidence in punitive administrative or criminal proceedings. For this contribution, we provide an overview of the Dutch framework.

4.1. Transfers of data between national proceedings

Similar to the gathering of information by administrative authorities, the Awb contains a general, albeit incomplete, framework for the subsequent processing of data by the relevant authorities. Neither the general framework nor sectorial legislation explicitly differentiates between ‘digital’ or ‘analogous’ information.

4.1.1. Sharing of information from administrative proceedings

General administrative law establishes a duty of official secrecy.¹⁶⁶ This duty is not absolute: it is limited to data collected in the exercise of an official’s task, and only data of a confidential nature that must be known or reasonably assumed is covered. This, for instance, includes personal data, medical data or data containing business secrets, but it will also cover

¹⁶⁴ AP Interview 05.03.2024.

¹⁶⁵ AP Interview 05.03.2024.

¹⁶⁶ Article 2:5 Awb.

information obtained under the threat of compulsion.¹⁶⁷ Official secrecy, therefore, can be said to contain a safeguard for citizens or economic actors. On the one hand, citizens or actors are under a legal obligation to provide information to administrative authorities in the performance of their tasks, but, on the other hand, they are given the guarantee that such information must be kept confidential, unless an exception to this duty exists.

In many sectorial areas, specific rules on official secrecy apply. The Belastingdienst is, for instance, subjected to a regime which is considered to be one of the most stringent in the Netherlands: every person is prohibited from disclosing anything which appears or is disclosed to them from or in connection with any activity in the implementation of the tax act concerning the person or affairs of any other person beyond what is necessary for the implementation of the tax act or for the collection of any state tax.¹⁶⁸ The duty of tax secrecy matters is considered to be so important, that it even applies in court proceedings. The Dutch financial supervisors have been subjected to specific rules of secrecy too.¹⁶⁹ The provisions serve as implementation of provisions of EU law and hold, in brief, that any person who performs or has performed any task by virtue of the application of financial supervision acts is prohibited from making further or other use of confidential information than as required for the performance of its duties or by these acts. In turn, information obtained in connection with any activity for the performance of ACM's tasks may be used only to the extent necessary for the performance of that task or of any other task referred to in Article 2(2).¹⁷⁰ This is different only where legislation so provides. Finally, the UAVG also contains some rules on the protection of confidential information.

Information that was collected in the exercise of administrative duties and that is of a confidential nature is to be kept secret, unless disclosure is necessary in light of a statutory duty to do so or because it is required for the exercise of an authority's duties. The latter exception prevents the duty of official secrecy from interfering with an authority's proper task performance as disclosure of confidential information may sometimes be necessary to realise that task.¹⁷¹ Consequently, confidential information may be shared for

¹⁶⁷ This argument is often made specifically in relation to official secrecy in tax matters, see B. van der Sar, *Fiscale geheimhoudingsplicht: art. 67 AWR ontrafeld*, Leiden, Netherlands, Leiden University, 2021, Chapter 3.2.0, with further references. There appears to be no convincing reason to restrict this argument to fiscal affairs alone.

¹⁶⁸ Article 67 AWR.

¹⁶⁹ Article 1:89 and following Wft.

¹⁷⁰ Article 7 ACM Establishment Act.

¹⁷¹ See R. Jacobs, 'Commentary 3 to Article 2:5' in T. Borman and J. de Poorter (eds), *Tekst & commentaar Awb*, Deventer, Netherlands, Kluwer, 2023.

the investigation, prosecution or judgment of criminal offences that relate directly to the area of competence of the administrative authorities.¹⁷²

In addition to rules on official secrecy and data protection, regard must be had to legal provisions that require administrative authorities to provide information to other authorities, either on their own motion or on request. For example, Article 55 AWR is regarded as a statutory exception to most, if not all other, duties of professional secrecy: the State's interest in levying taxes is considered to be so significant that it surpasses official secrecy, even in cases where this would not follow from the wording of the duty of secrecy itself. A similar exception applies to powers of criminal investigation – production orders, for instance – which, in principle, also supersede duties of secrecy unless the data requested falls within the scope of a legal professional privilege (see also Section 2.3.1.). Moreover, as regards criminal procedure, all authorities under public law are required, upon request of the public prosecutor, to provide any information concerning offences that have come to their knowledge during performance of their duties.¹⁷³ In addition to these general rules, sectorial legislation often provides specific exceptions to the base rule of official secrecy. For example, supervisors of the AFM should provide information to, *inter alia*, bodies entrusted with the exercise of powers of criminal procedure – e.g., investigating judges – if this is deemed necessary for the latter's tasks.¹⁷⁴ Furthermore, a supervisor can – spontaneously or upon request – provide to, *inter alia*, the prosecution service, the fiscal police, the Tax Administration, the ACM (in relation to payment services) as well as the AP (also in relation to payment services) to the extent that the provision of information is deemed necessary for the fulfilment of the task of the receiving authority.¹⁷⁵ As another illustration, the ACM is authorised to provide data to an administrative body, department, supervisor and other person charged with the detection of criminal offences, respectively the supervision of compliance with statutory regulations, if it has been determined by regulation of the Minister of Economic Affairs that the transfer is necessary for the proper performance of the receiving authority's task.¹⁷⁶ Consequently, it allows for the transfer of confidential data to all of the authorities in this study if necessary for the performance of their respective tasks. Note, however, that only information which reached the

¹⁷² The tax authorities, for instance, are competent to share information with the prosecution services or (fiscal) police for tax offences. This is considered to be a part of their statutory tasks, see HR 26.04.1988, ECLI:NL:HR:1988:AD5708, para 7.6.

¹⁷³ Article 162(2) WvSv. Interestingly, the financial supervisors have been exempted from this duty, see *Stb.* 1987, 141.

¹⁷⁴ Article 1:92(1) Wft.

¹⁷⁵ Article 1:93 Wft.

¹⁷⁶ Article 7(3)(a) ACM Instellingswet. See also Article 1 Regeling Gegevensverstrekking ACM 2019.

investigative dataset can be exchanged by the ACM with other authorities (see Section 3.1.4.).

It is noteworthy that an act that aims to provide a legal basis for data processing by partnerships of public and private organisations for the performance of a task of general interest has recently been adopted by the Dutch Parliament, and is set to enter into force in 2025.¹⁷⁷ This Act not only intends to strengthen the fight against fraud, but also to improve the possibilities of (personal) data sharing in cooperative ventures (*samenwerkingsverbanden*) engaged in tackling serious organised crime by creating common provisions for the sharing, processing and further transfer of data for all parties involved.¹⁷⁸

4.1.2. Sharing of evidence from criminal proceedings

Information that is obtained in criminal procedures can be transferred to administrative authorities for the fulfilment of their tasks, including punitive procedures. The relevant rules for the protection of personal data are laid down in statutory law: for the police (including specialised police services) in the Police Data Act and for the OM in the Judicial and Criminal Data Act (Wjsg).¹⁷⁹ We focus on the latter.¹⁸⁰

Article 39f Wjsg provides that the College of Prosecutors General can provide judicial data to persons or bodies for, *inter alia*, maintaining order and security, monitoring compliance with regulations, or taking an administrative decision. Such a transfer is possible only to the extent that it is necessary in view of an important public interest or the establishment, exercise or defence of a right in law, and is provided in such a form that redirection to persons other than the data subject is reasonably prevented.

¹⁷⁷ Wet van 19 juni 2024 tot regels omtrent gegevensverwerking door samenwerkingsverbanden (Wet gegevensverwerking door samenwerkingsverbanden), *Stb.* 2024, 198.

¹⁷⁸ Such common ventures have, for instance, existed for a longer period in the field of financial crime; similar developments are now taking place in other areas, too. Until now, such ventures did not alter the general and sectoral rules for official secrecy and data exchange, meaning that every time confidential information was shared, it had to comply with the specific legal rules of the providing and receiving actors. The proposed bill intends to facilitate the process of sharing of data, the further processing of it within such ventures, as well as the subsequent transfer of data to partners. See M. Luchtman, 'Samenwerkingsverbanden en de strafrechtspleging' *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2022, pp. 222-235.

¹⁷⁹ Both laws also serve to implement the provisions of Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties [2016] *OJEU* L 119/89.

¹⁸⁰ In this context, see De Vries (n. 17) pp. 246-247.

Decision-making powers are mandated to the relevant parts within the OM, and administrative authorities – including those which are studied in this contribution – can be designated as receiving parties.¹⁸¹ Each transmission is to be subjected to a proper balancing of interests *in concreto*. Moreover, the order clarifies that the relevant rules contain a discretionary power of the prosecution service and not a duty, as well as that transfers of judicial data may be possible *proprio motu* or upon request.

Article 39f Wjsg has been the subject of legal argument in cases which concern the transfer of intercepted telecommunication data from the Public Prosecution Service to the Dutch competition authorities, and the subsequent use of that data by the latter to impose administrative fines for violations of competition legislation on several legal persons.¹⁸² However, the administrative fine decisions were annulled as the District Court of Rotterdam considered the transfer of the intercepted data to breach the right to respect for private life (Article 8 ECHR).¹⁸³ In the absence of a knowable, reviewable balancing of interests by the Public Prosecution Service as part of the decision to transfer the evidence, compliance with Article 39f Wjsg could not be reviewed. As a result, the persons about whom the information was provided were not able to verify whether the interference with their privacy was justified. Before using data – especially if that data was obtained via intrusive investigative measures – the competition authorities should have ascertained why the public prosecutor considered that there was a substantial public interest and why the provision was necessary for that purpose. In appeal, however, the CBb annulled the judgment of the District Court and ruled that the impugned transfer of the data was not unlawful under the Wjsg nor in breach of Article 8 ECHR.¹⁸⁴ This outcome suggests that the (reasoning for the) transfer and use of data obtained through intrusive investigative measures on the basis of criminal law – including (traffic and location or content) data obtained from OSPs – will not be subjected to strict judicial scrutiny by Dutch courts.

Complaints before the ECtHR that the transmission of the tapped information had not been in accordance with the law and violated Article 8 ECHR have recently been dismissed.¹⁸⁵ The ECtHR accepted that the transmission to the competition authorities of data obtained through interception of telecommunication constitutes an interference with the

¹⁸¹ See *Aanwijzing Wet justitiële en strafvorderlijke gegevens*, Stcrt. 2018, 36059.

¹⁸² President District Court Den Haag 26.06.2009, ECLI:NL:RBSGR:2009:BJ0047

¹⁸³ District Court Rotterdam 13.06.2013, ECLI:NL:RBROT:2013:CA3079.

¹⁸⁴ CBb 09.06.2015, ECLI:NL:CBB:2015:193.

¹⁸⁵ ECtHR, *Janssen de Jong Groep B.V. and Others v. the Netherlands*, 16.05.2023, no. 2800/16 (referred to GC); ECtHR, *Burando Holding B.V. et Port Invest B.V. c. Pays-Bas*, 16.05.2023, no. 3124/16 and 3205/16.

plaintiffs' rights under Article 8 ECHR.¹⁸⁶ Yet, it also found that the applicable law – Article 39f Wjsg – did give the applicant companies an adequate indication of the circumstances and conditions under which the OM was empowered to resort to data transmission. Moreover, turning to the applicable safeguards, the ECtHR held that there was extensive *ex post facto* judicial oversight in place, as well as access to proceedings before the civil courts. In September 2023, the case was referred to the Grand Chamber of the ECtHR; it is expected that judgment will be delivered by the end of 2024. The case is interesting, because the ECtHR – as it notes itself – has not provided specific guidance before on the general precautions to be taken when communicating data obtained through interception of communications to other parties, except in specific contexts.

4.2. Transfers of data between foreign and national proceedings

The powers from the Awb or sectorial legislation are used to implement incoming requests for mutual administrative assistance from other (Member) States or EU agencies.¹⁸⁷ In turn, the Awb does not provide any rules on international and European mutual administrative assistance with authorities from other (Member) States, or EU bodies or agencies.¹⁸⁸ While information exchange is usually possible at the national level, the transfer of data to other jurisdictions follows the traditional rules of mutual administrative assistance. This usually implies that data is only transferred to foreign authorities that perform comparable tasks. Should those data later turn out to be of relevance for purposes of criminal investigation or prosecution or other areas of administrative enforcement, permission of the transferring authority to do so is usually required. When information is transferred to foreign police or prosecution services, it is not uncommon that permission is required from the Dutch Ministry of Justice and Security; some Dutch statutes (e.g., the Wft) are more specific on this than others. Dutch sectoral regulations show quite a significant degree of divergence, as mutual administrative assistance is not covered by the Awb.

Additionally, Dutch authorities may be required to exchange information with EU authorities or authorities established in other Member States on the basis of sector specific EU legislation. In the area of competition law, for example, the exchange of information with administrative authorities in other Member States or the EU Commission is specified in Council Regulation 1/2003 and Directive 2019/1. Article 7 of the ACM Establishing

¹⁸⁶ See by contrast ECJ, *WebMindLicences*, 17.12.2015, C-419/14, § 79.

¹⁸⁷ See eg De Vries (n. 17) pp. 219 and followings.

¹⁸⁸ See Boswijk, Jansen and Widdershoven, 'De wettelijke implementatie van administratieve samenwerking in de Europese Unie' (n. 17) p. 323.

Act reiterates this and prescribes several conditions for the exchange of information with foreign institutions. Firstly, the confidentiality of the information needs to be sufficiently guaranteed, and, secondly, it needs to be sufficiently guaranteed that the information is not being used for a purpose other than that for which the information was provided.¹⁸⁹ The ACM assesses both requirements on the basis of an internal working method.¹⁹⁰ Another relevant example forms the exchange of information among data protection authorities established in different Member States and/or with the European Data Protection Board, as required under the GDPR.¹⁹¹ Such information exchanges take place via the EU's Internal Market Information system, which allows data protection authorities to submit mutual assistance requests and/or organise joint operations. Such requests can either be formally – which cannot be refused unless the data protection authority is not competent for the subject matter of the request or compliance with the request would infringe EU or national law¹⁹² – or voluntary. This voluntary request does not impose a binding obligation upon a data protection authority, and can therefore be ignored.¹⁹³

4.3. Admissibility of data collected from online service providers as evidence

Under Dutch law, there are no specific rules that determine the admissibility of data collected from third parties, such as OSPs, as evidence in criminal and punitive administrative proceedings. The general rules apply. For this contribution, we provide a brief overview of the relevant rules of evidence in the Netherlands.

4.3.1. Use of data as evidence in (punitive) administrative proceedings

The guiding principle of Dutch administrative law of evidence is the so-called free evidence doctrine (*vrije bewijsleer*). This doctrine means that 'administrative law courts have much discretion as far as evidence is concerned: this relates to questions about the scope of evidence, the division of the burden of proof, means of evidence and the appreciation of evidence

¹⁸⁹ ACM Instellingswet, Article 7(4).

¹⁹⁰ ACM Interview 08.02.2024.

¹⁹¹ The obligation to exchange information stems from the general obligation for data protection authorities to reach consensus on the outcome on an enforcement case where the alleged infringement took place in a cross-border context, See Article 60 of the GDPR.

¹⁹² Article 61(4) GDPR.

¹⁹³ L Mustert, *Cross-border enforcement of the GDPR by independent administrative authorities*, doctoral thesis, University of Luxembourg, 2023, <https://orbilu.uni.lu/handle/10993/55782>.

by the courts'.¹⁹⁴ This does, however, not mean that relevant safeguards derived from international or EU fundamental rights can be ignored: the use of unlawful evidence in administrative proceedings is precluded in cases wherein evidence is obtained in a way that runs so counter to what may be expected of a properly acting administrative authority that the use of evidence should be considered inadmissible in all circumstances (see also Section 2.4.1.). The 'manifestly improper' criterion is used when administrative courts are required to assess whether evidence which was gathered unlawfully during administrative or criminal procedures can be used in punitive administrative procedures. What has been declared inadmissible in criminal procedures is not automatically inadmissible in administrative procedures; administrative courts determine and interpret the relevant facts and legal rules autonomously in accordance with their own procedural laws.¹⁹⁵ The manifestly improper criterion is also used to deal with irregularities that have allegedly been committed abroad,¹⁹⁶ at least in cases where the disputed investigative acts were conducted by Dutch administrative authorities.¹⁹⁷

In the context of the admissibility of evidence gathered by foreign administrative authorities, officials stressed that such evidence may only be used where the information has been collected in a way which respects the same level of protection of the rights of defence of natural persons as provided for under the national rules of the receiving authority.¹⁹⁸ As an example, ACM officials are therefore, in principle, required to assess each time whether the received information was collected in a way which respects the same level of protection of the Dutch defence rights. ACM officials confirm that this is usually checked, but that this never had led them to conclude that information could not be used to impose sanctions.¹⁹⁹

4.3.2. Use of digital data as evidence in criminal proceedings

Several recent studies have already provided a detailed description and analysis of the rules of Dutch criminal procedure regarding the admissibility of evidence in criminal proceedings, including the use of 'administrative' and

¹⁹⁴ This section is largely based on Duijkersloot, De Vries and Widdershoven (n. 73) p. 199.

¹⁹⁵ This approach follows from the fact that both areas of law serve different goals and follow different procedures.

¹⁹⁶ Duijkersloot, De Vries and Widdershoven (n. 73) pp. 205 and followings with further references. See also De Vries (n. 17) pp. 270-271.

¹⁹⁷ CRvB 01.10.2018, ECLI:NL:CRVB:2018:2911.

¹⁹⁸ Regulation 1/2003, Article 12(3). See also AP Interview 5.3.2024.

¹⁹⁹ ACM Interview 08.02.2024.

‘foreign’ evidence.²⁰⁰ In short, written administrative evidence and reports that have been drawn up by foreign officials or officials of EU or international organisations qualify as evidence in criminal proceedings.²⁰¹ Digital evidence can be used in Dutch criminal proceedings; the nature, the contents and/or an analysis of the data collected throughout the investigation is generally described in reports included in the case file. While digital evidence is, in principle, admissible, there can be grounds to question its reliability, or the reliability of the inferences made from the digital evidence. Equality of arms is an important rule to allow the defence to test and challenge digital evidence and/or the inferences made from it. Debates as to the extent of disclosure necessary to assess the reliability of digital evidence are not uncommon, especially in cases in which the evidence has been (partly) gathered in other countries.²⁰²

With regard to unlawfully obtained or transferred (digital) evidence, Dutch legal practice seems to correspond to the case law of the ECtHR. Unlawful evidence is not inadmissible as such, but whether procedural consequences (e.g., a lower sanction or exclusion of the evidence) must be attached to breaches is reviewed by the trial court based on Article 359a WvSv. The scope of protection of Article 359a WvSv is, in principle, limited to alleged irregularities that have taken place in the criminal investigation into the charged offences; breaches that occurred in administrative investigations will usually fall outside the scope of this provision.²⁰³ It is consequently assumed – as long as there is no case law – that unlawfully obtained or transferred materials in administrative procedures will only lead to procedural sanctions in criminal procedures if the authorities have obtained the evidence in a manner that is ‘manifestly improper in light of what can be expected of a

²⁰⁰ This section is based on J. Lindeman, M. Luchtman and D. van Toor, ‘Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair-Trial Rights in the Netherlands’ in L. Bachmaier Winter and F. Salimi (eds), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings Electronic Evidence, Efficiency and Fair Trial Rights*, Oxford, United Kingdom, Hart, 2024 (forthcoming). See also De Vries (n. 17) pp. 250 and followings; Duijkersloot, De Vries and Widdershoven (n. 73) p. 202.

²⁰¹ Article 344(1)(3) WvSv.

²⁰² See HR 13.06.2023, ECLI:NL:HR:2023:913 (*Encrochat I*) and HR 13.02.2024, ECLI:NL:HR:2024:192 (*Encrochat II*).

²⁰³ Only in exceptional circumstances may legal consequences be attached to procedural errors that were not committed during the preliminary criminal investigation. This is the case when such errors have had a ‘decisive influence’ on the course of the investigation into and/or (further) prosecution of the suspect for the offence charged. Article 359a WvSv will then be then applied analogously, see HR 01.12.2020, ECLI:NL:HR:2020:1890; HR 13.06.2023, ECLI:NL:HR:2023:913 (*Encrochat I*); HR 13.02.2024, ECLI:NL:HR:2024:192 (*Encrochat II*).

properly acting public authority’, and, therefore, that the use of the evidence should be considered inadmissible in all circumstances.

In relation to evidence that was *unlawfully* obtained in or transferred from *abroad*, Dutch courts are not required to test the lawful gathering or transfer of evidence on the basis of foreign law or Article 8 ECHR if those materials were collected under the responsibility of foreign authorities of a State which is a Party to the ECHR.²⁰⁴ The task of Dutch criminal courts is limited to ensuring that the manner in which the results of this investigation are used in the criminal case does not violate the suspect’s right to a fair trial. The latter means, according to the Supreme Court, that the judge only pays attention to how those results were obtained if it is relevant to assessing whether the use as evidence of the results is consistent with the right to a fair trial.²⁰⁵ Where the *reliability* of investigation results used for foreign evidence is concerned, courts may only use evidence they consider reliable and useful. There may be grounds for exclusion of evidence if irregularities have occurred that have substantially affected the reliability and accuracy of investigation results. In this regard, there is no principle difference between situations wherein those investigation results were obtained under the responsibility of foreign authorities or in a Dutch criminal investigation. Criminal courts may take as a starting point that investigations carried out under the responsibility of foreign authorities were conducted in such a way that the results obtained by those investigations are reliable. Only if there are concrete indications to the contrary, are courts obliged to examine the reliability of those results.²⁰⁶

5. CONCLUSION

In this contribution, we have assessed the applicable framework regarding the gathering of digital evidence in punitive administrative proceedings in the Netherlands, with a specific emphasis on the options and limits of obtaining such evidence from third parties, specifically OSPs, and the sharing and use of such evidence at the interface of administrative and criminal enforcement. On the basis of our assessment, we would provide the following concluding remarks concerning the gathering of digital evidence in punitive administrative proceedings in the Netherlands.

²⁰⁴ See De Vries (n. 17) pp. 260-261. This is only different if it has been irrevocably established in the country concerned that the investigation was not carried out in accordance with the applicable rules of law. Dutch criminal courts must then assess whether that irrevocable finding gives cause to attach a legal consequence to the omission in question under (the analogous application of) Article 359a WvSv, see HR 13.06.2023, ECLI:NL:HR:2023:913 (*Encrochat I*), 6.5.2.

²⁰⁵ HR 13.06.2023, ECLI:NL:HR:2023:913 (*Encrochat I*), 6.5.4.

²⁰⁶ HR 13.06.2023, ECLI:NL:HR:2023:913 (*Encrochat I*), 6.6.

The applicable Dutch legal framework on the basis of general administrative law (Awb) and/or sectorial legislation (e.g., AWR, ADW, and Wft) does not feature specific supervision powers for the gathering of digital evidence. Instead, the ‘regular’ powers to demand information, inspect business records and documents, and access to professional locations are relied upon with regard to the gathering of ‘analogous’ evidence as well as digital evidence. Several Dutch administrative authorities have adopted their own sector-specific approach to deal with current questions relating to digital evidence, most notably the ‘filtering’ of private or privileged information from datasets.

While Dutch administrative law technically allows information demands against third parties, it seems that demands against OSPs are quite rare in practice in most fields. In our view, there are two main reasons for this (in addition, perhaps, to the aforementioned lack of a specific legal basis to make such demands). The first reason is that doctrine and statutory law dictate that the implementation of administrative action, including the use of supervisory powers, should comply with the general principles of good administration, including proportionality. Compliance with general principles of good administration is subjected to *ex post* judicial review by the administrative courts. Demands against third parties, including OSPs, should be proportionate, and recent case law suggests that it may be disproportionate to demand information from an OSP in administrative proceedings, also in light of the right to private life of the person concerned. The second reason is that in the Dutch legal order, intrusive and covert investigative measures are, as a rule, reserved exclusively for criminal proceedings under the auspices of the OM. This means that, in practice, serious breaches of substantive legislation that require intrusive or covert measures – e.g., access to traffic and location data or interception of telecommunication – to investigate the case shall be reported to the OM by the administrative authorities. In the selected substantive policy fields, criminal investigations will be performed by the special investigation service FIOD.

Despite the existence of duties of professional secrecy on the basis of (general or sectorial) administrative law and criminal law, there are many provisions that allow digital evidence to be shared between the administrative and judicial authorities, provided that the statutory requirements are fulfilled. In turn, administrative evidence can be used for the purpose of criminal investigations, and evidence that was obtained during criminal investigations can also be relied upon for the purpose of punitive administrative proceedings. The options to obtain judicial review of administrative action (or, for that matter, measures taken on the basis of criminal procedural law) are limited in the Dutch legal order. Save for the option of launching interim relief proceedings before civil courts, it is only possible to appeal

administrative action, including the implementation of supervisory powers, *ex post* if and in so far, such action is relevant with regard to a subsequent administrative decision. As part of their scrutiny, Dutch administrative courts will review compliance with general principles of good administration, including proportionality, the requirements of statutory law, and fundamental rights standards concerning, *inter alia*, the right to a fair trial and the right to private life. In accordance with Dutch case law, evidence must be excluded from the administrative proceedings if it has been obtained in a manner that is ‘manifestly improper’. With regard to digital evidence, case law shows that the gathering of digital evidence by administrative authorities without an applicable specific legal basis to do so or the disproportionate use of supervisory powers to gather evidence from third parties may require the exclusion of the evidence.

12. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN POLAND

K. KASZUBOWSKI and S. STEINBORN

1. COMPETENT AUTHORITIES IN SELECTED AREAS OF PUNITIVE ADMINISTRATIVE ENFORCEMENT

Administrative financial penalties (administrative fines) are imposed on persons or entities that have violated administrative regulations, for instance, on the rules of conducting a certain activity, environmental protection requirements. An administrative fine is transversally defined at Article 189b of the Code of Administrative Proceedings (CAP).¹ According to this definition, an administrative fine is understood as a monetary sanction specified by law, imposed by a public administration, through a decision, following a breach of the law consisting of a failure to fulfil an obligation or a breach of a prohibition, imposed on a natural person, a legal person or an organisational unit without legal personality.

Unlike criminal penalties, administrative penalties are not retributive sanctions imposed for the commission of criminal offences. Rather, they serve as coercive measures intended to enforce compliance with administrative law.² Nonetheless, the severity of administrative penalties may, in certain cases, exceed that of criminal penalties, particularly in terms of their monetary amount. It is therefore essential to distinguish administrative penalties from criminal sanctions, both in terms of the nature of the violation

¹ Law of 14.06.1960 – Code of Administrative Proceedings (*Kodeks postępowania administracyjnego*), consolidated text: Journal of Laws 2024, item 572. Financial penalties in the area of customs law may be imposed for failure to make an INTRASTAT declaration or failure to make a correction of it (Article 101 CL) or for breaches of provisions of regulation (EU) 952/2013 of the European Parliament and of the Council of 9.10.2013 laying down the Union Customs Code (OJ EU of 10.10.2013 L No 269, p. 1).

² See more M. Lewicki, 'Pojęcie sankcji prawnej w prawie administracyjnym' *Państwo i Prawo*, 2002, no. 8, p. 65 et seq.; A. Wróbel, 'Odpowiedzialność administracyjna w orzecznictwie Trybunału Konstytucyjnego (na przykładzie administracyjnych kar pieniężnych)', *Europejski Przegląd Sądowy*, 2014, no. 9, p. 33 et seq.

and the procedural framework through which they are imposed. Criminal penalties can only be imposed for criminal offences by decision of courts in criminal proceedings, whereas administrative penalties are imposed after administrative proceedings by administrative authorities. These latter decisions are subject to review by administrative courts and therefore only for legality³. However, some administrative authorities empowered to impose such penalties may also exercise functions typically associated with criminal authorities, particularly when authorised by law to investigate criminal offences falling within their area of competence.

1.1. Customs authority

The authority empowered to impose administrative penalties for breaches of the customs law (CL)⁴ is the Head of the Customs and Fiscal Office (*naczelnik urzędu celno-skarbowego*), as the body of first instance, and the Director of the Chamber of Fiscal Administration (*dyrektor izby administracji skarbowej*) as the second instance body in case of appeal of the decisions of the Head of the Customs and Fiscal Office.⁵ Proceedings conducted by both instances, including those concerning the imposition of an administrative fine, have the nature of administrative proceedings. The provisions of the Tax Ordinance (TO)⁶, notwithstanding the differences resulting from the provisions of the CL⁷, are applied accordingly.

The Customs and Fiscal Office is also authorised to conduct pre-trial proceedings in cases of fiscal criminal offences relating to breaches of customs obligations⁸. It is also authorised to bring an indictment before courts in such cases.⁹ In that case, the Office appears before courts acting as a public prosecutor. Importantly, however, proceedings concerning the imposition of an administrative penalty are entirely separate from criminal proceedings, even when both are conducted by the same authority.

³ Article 3 § 2 (1) of the Law of 30.08.2002 on proceedings before administrative courts (*Prawo o postępowaniu przed sądami administracyjnymi*), consolidated text: Journal of Laws 2024, item 935 as amended.

⁴ Law of 19.03.2004 – Customs Law (*Prawo celne*), consolidated text: Journal of Laws 2024, item 1373.

⁵ Article 69 CL.

⁶ Law of 29.08.1997 – Tax Ordinance (*Ordynacja podatkowa*), consolidated text: Journal of Laws 2025, item 111.

⁷ Article 73 CL.

⁸ Article 118 § 1 and Art. 133 § 1 p. 1 Penal Fiscal Code (PFC).

⁹ Article 155 § 4 PFC in conjunction with Article 53 § 37 PFC.

1.2. Tax enforcement as regards VAT

The authorities competent to impose administrative penalties for VAT breaches are the two Tax Authorities: the Head of the Tax Office (*naczelnik urzędu skarbowego*) and the Head of the Customs and Fiscal Office (*naczelnik urzędu celno-skarbowego*). The proceedings conducted by these authorities, including the imposition of these penalties, are administrative proceedings conducted based on the Tax Ordinance. The Tax Office, as the Customs and Fiscal Office, can also conduct pre-trial proceedings in cases of fiscal criminal offences related to VAT and to bring charges to criminal courts as a public prosecutor.

The Value Added Tax Act (VAT Act)¹⁰ contemplates several administrative penalties that the Tax Authorities may impose on taxpayers.¹¹ Penalties may be imposed, for instance, in the case of violations of obligations relating to the recording of sales and requirements relating to cash registers. In the event of an understatement of the tax liability or of making sales without the use of a cash register, the Tax Authorities can impose an additional penalty on the VAT taxpayer in a fine of 30% of such amount.¹² In case where the taxpayer knowingly participates in tax fraud and derives unauthorised financial benefits, an additional fine of 100% of the tax can be imposed.¹³

In view of the circumstances in which these additional penalties can be imposed, they do not constitute an individual tax increase but are rather repressive in nature, as they penalise those who fail to comply with VAT obligations. They can also, therefore, be classified as a fiscal (administrative) penalty,¹⁴ as recognised by the case law of the European Court of Justice (ECJ)¹⁵ and of national administrative courts.¹⁶

¹⁰ Law of 11.03.2003 on tax on goods and services (*Ustawa o podatku od towarów i usług*), consolidated text: Journal of Laws 2024, item 361 as amended.

¹¹ Article 109 sec. 3h, Article 111 sec. 6j and 6ka, and Article 145a sec. 8 and 10 VAT Act.

¹² Article 112b and Article 111 sec. 2 VAT Act.

¹³ Article 112c VAT Act.

¹⁴ R. Bulejak, in: I. Ożóg (ed.), *Karuzele i inne oszustwa podatkowe. Metody przeciwdziałania unikaniu opodatkowania*, Warszawa, Poland, Wolters Kluwer Polska, 2021, pp. 254, 334; J. Pachecka, M. Gizicki, 'Sankcje grożące za unikanie opodatkowania', p. 400, in: D.J. Gajewski (ed.), *Uszczelnienie systemu podatkowego w Polsce*, Warszawa, Poland, Wolters Kluwer Polska, 2020; K.J. Musiał, 'Dlaczego rak nie jest rybą, czyli słów parę o sankcji VAT i ostatnich perturbacjach z nią związanych' *Przegląd Podatkowy*, 2023, no. 6, p. 17 et seq.; D. Zalewski, in: D. Zalewski (ed.), *Kary pieniężna nakładane przez KAS i ich zaskarżanie*, Warszawa, Poland, Wolters Kluwer Polska, 2021, pp. 265-266.

¹⁵ ECJ, *Grupa Warzywna Sp. z o.o. v. Dyrektor Izby Administracji Skarbowej we Wrocławiu*, 15.04.2021, C-935/19, EU:C:2021:287.

¹⁶ Resolution of the Supreme Administrative Court of 16.10.2006, I FPS 2/06, LEX No. 200105; judgment of the Supreme Administrative Court of 28.08.2008, I FSK 972/07, LEX No. 469028.

1.3. Punitive enforcement in the area of banking law and financial markets

According to the Law on Financial Market Supervision (LFMS),¹⁷ the supervision of the financial market is conducted by the Financial Supervision Commission (*Komisja Nadzoru Finansowego*, FSC), led by the Chairman of the Commission. The Chairman also heads the Office of the FSC, which provides support for the Commission's activities. The FSC is a collegiate body whose main task is to oversee the proper functioning of the entire financial market in Poland. Financial market supervision encompasses, *among other things*, banking supervision, supervision of open-ended pension funds, insurance supervision, capital market supervision, and payment institution supervision.¹⁸

The FSC is both an executive power authority and a public administration authority, which, however, is not part of the government,¹⁹ as decided by the Constitutional Court (*Trybunał Konstytucyjny*), as its status is characterised by considerable independence and autonomy, greater than other regulatory administrative bodies.²⁰ The Prime Minister only supervises the activities of the Office of the FSC.²¹

Within its supervisory competence, the FSC can impose administrative fines on supervised entities if they breach the obligations set out in the LFMS or under EU law. The power to impose administrative fines on supervised entities is vested exclusively in the FSC and cannot be exercised by the Chairman of the Commission, their deputies or the staff of the Commission Office.²²

To determine whether there are grounds for filing a notice of suspicion of a criminal offence or for initiating administrative proceedings for the violation of the provisions of the LFMS within the scope of the FSC's supervision, the Chairman may order the opening of an investigation. The purpose of such an investigation is to gather information on the circumstances concerning a specific alleged violation of the relevant provisions by

¹⁷ Law of 21.07.2006 on Financial Market Supervision (*Ustawa o nadzorze nad rynkiem finansowym*), consolidated text: Journal of Laws 2024, item 135 as amended.

¹⁸ Article 1 sec. 2 LFMS.

¹⁹ A. Nadolska, *Komisja Nadzoru Finansowego w nowej instytucjonalnej architekturze europejskiego nadzoru finansowego*, Warszawa, Poland, Wolters Kluwer Polska, 2014, p. 245.

²⁰ Judgment of the Constitutional Court of 15.06.2011, K 2/09, OTK-A 2011, no. 5, item 42; A. Nadolska (n. 21), pp. 259-260.

²¹ Article 3 sec. 3 LFMS.

²² Article 12 LFMS.

supervised financial institutions.²³ The Commission aims to collect as many documents and information as possible to assess whether the activities of a specific entity may constitute a possible violation of the law.²⁴ Once relevant material is collected and evidence is found of an infringement, proceedings may be initiated before the Commission, which may impose an administrative financial penalty on the supervised entity.

The investigation procedure is autonomous in nature and, by exception, the provisions of the Code of Administrative Proceedings (CAP) do not apply, unless the provisions of the Financial Market Supervision Act explicitly stipulate otherwise.²⁵ The result of the investigation can be both the initiation of an administrative proceeding leading to imposing an administrative fine and/or the filing of a criminal offence notice. The FSC, therefore, has mixed competences: investigative and administrative.

1.4. Competition law enforcement

Pursuant to Article 29 sec. 1 of the Law on Competition and Consumer Protection (CCPL),²⁶ the President of the Office of Competition and Consumer Protection (*Prezes Urzędu Ochrony Konkurencji i Konsumentów*, OCCP) is the central governmental administrative body competent in matters of competition and consumer protection. The CCPL allows the President of the Office to impose administrative fines on supervised entities for violations of competition provisions.

The CCPL regulates administrative proceedings before the President of the OCCP, including those involving the imposition of fines for competition infringements.²⁷ To the extent not regulated in the CCPL, the provisions of Article 227-315 of the Code of Civil Proceedings (CCivP)²⁸ concerning evidence in civil proceedings apply accordingly.²⁹

²³ See P. Karlik, 'Postępowanie wyjaśniające przez Komisję Nadzoru Finansowego a gwarancje procesowe jego uczestników' *Przegląd Prawa Handlowego*, 2024, no. 1, p. 33; M. Burgiel-Bosak, 'Zasady i tryb postępowania wyjaśniającego prowadzonego przez Komisję Nadzoru Finansowego – zagadnienia wybrane' *Monitor Prawa Bankowego*, 2016, no. 11, p. 67.

²⁴ P. Karlik (n. 26), p. 34.

²⁵ Article 18a sec. 1 LFMS.

²⁶ Law of 16.02.2007 on Competition and Consumer Protection (*Ustawa o ochronie konkurencji i konsumentów*), consolidated text: Journal of Laws 2024, item 1616.

²⁷ Article 85 CCPL.

²⁸ Law of 17 November 1964 - Code of Civil Proceedings (*Kodeks postępowania cywilnego*), consolidated text: Journal of Laws 2024, item 1568 as amended.

²⁹ Article 84 CCPL.

1.5. GDPR enforcement

Proceedings for violations of the provisions on the protection of personal data and the imposition of related administrative fines are conducted by the President of the Personal Data Protection Office (*Prezes Urzędu Ochrony Danych Osobowych*, PDPO), as regulated under Articles 60 and 101 of the Law of 10.05.2018 on personal data protection (PDPL).³⁰ The provisions of the CAP shall apply in matters not regulated therein. Proceedings before the President of the PDPO are single-instance proceedings, and the President's decision is subject to complaint to the administrative court.³¹

Proceedings conducted by the President of the PDPO regarding the infringement of provisions on personal data protection and the imposition of administrative fines have the nature of administrative proceedings³². The President of the PDPO has powers of an investigative nature in this respect, although he is an administrative body, and the proceedings conducted by him have the nature of administrative proceedings.

2. PUNITIVE ADMINISTRATIVE PROCEEDINGS: GENERAL FRAMEWORK

Pursuant to the CAP, administrative fines are imposed in proceedings conducted by public administrative bodies, either central or local.³³ However, the provisions of the CAP regarding administrative fines³⁴ do not contain any specific regulations concerning proceedings, including evidentiary provisions. Indeed, the CAP only regards the imposition of administrative fines and their amendment at the stage of execution, so there are only regulations of substantial legal nature.³⁵

³⁰ Law of 10.05.2018 on personal data protection (*Ustawa o ochronie danych osobowych*), consolidated text: Journal of Laws 2019, item 1781 as amended.

³¹ Article 7 sec. 2 CCPL.

³² See P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa, Poland, Wolters Kluwer Polska, 2022, p. 801; J. Łuczak-Tarka, in: D. Lubasz (ed.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa, Poland, Wolters Kluwer Polska, 2019, pp. 493-494.

³³ Article 1 sec. 1 and 2 CAP. On the concept of a public administration body - see: W. Chróścielewski, in: J. Chlebny, W. Chróścielewski, P. Dańczak, et al., *Zakres przedmiotowy i podmiotowy administracyjnego postępowania ogólnego. System prawa administracyjnego procesowego. Tom II. Część I*, Warszawa, Poland, Wolters Kluwer Polska, 2018, p. 124 et seq.

³⁴ Section IV A, Art. 189a-189j CAP.

³⁵ B. Adamiak, in: B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa, Poland, C.H. Beck, 2017, p. 951; K. Ziemiński, 'Próba oceny trafności objęcia Kodeksem postępowania administracyjnego możliwości stosowania sankcji karnych przez administrację', pp. 401-402, in: W. Chróścielewski, Z. Kmiecik (eds.), *Idea*

There is no definition of ‘electronic evidence’ in the CAP, nor any specific regulation for its gathering, including from Online Services Providers (OSPs). The CAP only expressly provides for the possibility for administrative authorities to communicate with the parties and settle matters electronically³⁶.

The evidentiary proceedings are conducted by administrative authorities, which are free to determine their scope. Proceedings follow the adversarial principle. If the party decide to exercise it, they may participate in the activities of the evidentiary proceedings, express their opinion as regards the evidence collected and used, as well as submit motions for the performance of specific evidence or present it independently.³⁷ Requests to accept evidence are not binding for the administrative body conducting the proceedings.³⁸ It may disregard them if the circumstances relevant to the case are sufficiently established by other evidence³⁹ or if there are insufficient arguments to challenge the findings previously established.⁴⁰ Administrative authorities should adhere to the principle of proportionality⁴¹ and use evidence that is appropriate to the purpose it is intended to serve. Evidence should be adequate to the nature and subject matter of the facts being proved.⁴²

It follows from the above that, for the purposes of administrative proceedings, data may be obtained from various entities, including OSPs, as long as it is useful for resolving the case. Importantly, however, the selected legal frameworks do not provide administrative authorities with any legal means to mandate a specific entity to provide evidence. This applies to any party or any other participants in administrative proceedings, as well as third parties. Only Article 7b CAP provides for the principle of cooperation of administrative authorities as a general principle of proceedings. Still, it applies only to the collaboration between administrative authorities, to the

kodyfikacji w nauce prawa administracyjnego procesowego. Księga pamiątkowa Profesora Janusza Borkowskiego, Warszawa 2018.

³⁶ Article 39 § 1, Art. 63 § 1 CAP.

³⁷H. Knysiak-Molczyk, *Uprawnienia strony w postępowaniu administracyjnym*, Kraków, Polska, Kantor Wydawniczy Zakamycze 2004, pp. 147-177.

³⁸ Article 78 CAP.

³⁹ Judgment of the Supreme Administrative Court of 21.07.2016, I FSK 808/16, LEX No. 2100301.

⁴⁰ Judgment of the Voivodship Administrative Court Warsaw of 9.12.2022, VI SA/Wa 2210/22, LEX No. 3501840.

⁴¹ Article 8 CAP.

⁴² R. Suwaj, *Zasady nakładania kar administracyjnych*, Warszawa, Poland, Wolters Kluwer Polska, 2021, pp. 121-122, 123.

extent necessary for the thorough clarification of the factual and legal state of the case (see Section 4.1).⁴³

Therefore, OSPs may provide data to administrative authorities voluntarily, unless restrictions arise from other regulations, such as those related to telecommunications or commercial confidentiality. Administrative authorities, therefore, do not have the possibility to compulsorily obtain data from OSPs.

OSP, under Polish law, are defined in Article 2 sec. 6 of the Electronic Communications Law (ECL)⁴⁴, based on EU law.⁴⁵ It stipulates, on one hand, that a provider of electronic communication services is a provider of publicly available telecommunications services or an entity providing publicly available interpersonal communication services not using numbers. On the other hand, an electronic communication service is a service provided *via* a telecommunications network, usually for remuneration, excluding services related to the provision or exercise of control over content transmitted using telecommunications networks or electronic communication services, including an Internet access service, an interpersonal communication service and a service consisting wholly or mainly in the transmission of signals, in particular the transmission of signals as part of interpersonal communication regardless of the technology used, a transmission service used to provide machine-to-machine communication services and for broadcasting.⁴⁶ These definitions, due to the nature of the ECL, can be considered to encompass all kinds of OSPs.

3. PUNITIVE ADMINISTRATIVE PROCEEDINGS: SECTORAL FRAMEWORK

3.1. Requests for data to online service providers

3.1.1. Customs enforcement

The customs legislation does not provide a specific provision for the collection of data from third parties by the customs authority. The provisions of the Tax Ordinance as amended by the Customs Law⁴⁷ shall apply *mutatis mutandis* to customs proceedings, which include the provisions on evidence (see Section 3.1.2).

⁴³ Judgment of the Supreme Administrative Court of 10.11.2021, III FSK 4168/21, LEX No. 3294685.

⁴⁴ Law of 12.07.2024 – Electronic Communications Law (*Prawo komunikacji elektronicznej*), Journal of Laws 2024, item 1221.

⁴⁵ Article 2 sec. 4 of Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code.

⁴⁶ Article 2 point 76 ECL.

⁴⁷ Article 73 CL.

3.1.2. Tax enforcement as regards VAT

The Tax Ordinance does not contain any provision on administrative fines. The application of the Tax Ordinance to administrative pecuniary penalties may result from Article 189a § 2 CAP⁴⁸ or other explicit provisions. However, Article 189a § 2 CAP assumes that in proceedings concerning administrative fines, the provisions of the Tax Ordinance should apply, particularly the prerequisites for assessing an administrative fine.

There are no specific regulations on electronic evidence in the Tax Ordinance. Their admissibility results, as in administrative proceedings, from the principle of an open catalogue of means of evidence and the definition of evidence. Under Article 180 § 1 TO, everything that may contribute to clarifying the case and is not contrary to the law should be admitted as evidence. This regulation supplements Article 181 TO, containing an exemplary catalogue of evidence in tax proceedings. It indicates that evidence in tax proceedings may be, in particular, tax books, declarations submitted by a party, testimonies of witnesses, expert opinions, materials and information collected as a result of inspection, tax information and other documents collected in the course of analytical activities of the National Fiscal Administration, inspection, tax control or customs and fiscal control, as well as materials collected in the course of criminal proceedings or proceedings in cases of fiscal offences or fiscal contraventions.

The evidentiary proceedings are conducted by the tax authority, which is free to determine their scope. Parties have the right to participate in these proceedings and if they choose to exercise this right, may participate in evidentiary actions, express their opinion as to the evidence carried out, submit motions for the taking of certain evidence or present it independently. Requests for the taking of evidence are not binding on the administrative authority. The party's request for the taking of evidence should be accepted if the subject of evidence is circumstances which are significant for the case, unless those circumstances are sufficiently established by other evidence.⁴⁹

The tax authority has no legal means by which it could ‘compel’ a third party to make evidence available in proceedings concerning administrative fines. The only exception is during ongoing tax proceedings in which there is a need to supplement evidence or compare it with information from other entities. In such cases, the Tax authorities may compel certain entities (for instance, banks, insurance companies, investment funds, and others) to provide information⁵⁰. Due to the limited scope of this provision, which only

⁴⁸ Cf. R. Suwaj (n. 46), pp. 63-65.

⁴⁹ Article 188 TO.

⁵⁰ Article 182 TO.

applies to tax proceedings, this rule does not extend to proceedings regarding the imposition of an administrative penalty.

3.1.3. Punitive enforcement in the area of banking law and financial markets

The investigation that the Chairman of the FSC may order is undoubtedly of an investigative nature. Among its investigative powers, searches can be carried out on the premises of the entity whose activities are related to the investigation, and the employee of the FSC carrying out the search may even be assisted by the Police in this respect.⁵¹ In the course of these proceedings, to the FSC can also seize documents or carriers of information, but only from the entity whose activities are related to these proceedings or its employees. Therefore, the investigation focuses exclusively on the controlled entity, and it is not possible to obtain evidence, including electronic evidence, from third parties.

The LFMS do not provide for any specific provisions regarding the proceedings conducted by the FSC for imposing administrative fines. Therefore, the CAP applies to the proceedings of the Commission and before the Commission (see Section 2).⁵²

3.1.4. Competition law enforcement

In competition proceedings, the provisions of the CCivP apply, including on documentary evidence.⁵³ According to this provision, everyone is obliged to present, within a specified period, a document in their possession and constituting evidence of a fact relevant to the outcome of the case, unless the document contains classified information. The case law emphasises that this provision covers the obligation to produce an existing, concrete document that constitutes evidence of a fact relevant to the outcome of the case, rather than the production of a new one. It does not, therefore, provide a basis for obliging a third party to produce a document, to compile certain information or to search for unspecified documents that could be used in the process.⁵⁴ This obligation to present documents applies to everyone,⁵⁵ including third parties such as OSPs. This obligation does not apply to persons who could refuse to testify regarding information covered by the document.⁵⁶

⁵¹ See P. Karlik (n. 26), p. 34.

⁵² Article 11 sec. 5 LFMS.

⁵³ Article 248 CCivP.

⁵⁴ See the decision of the Supreme Court of 30.06.2022, I CSK 1409/22, *Orzecznictwo Sądów Polskich*, 2023, no. 10, item 76.

⁵⁵ Article 248 § 1 CCivP.

⁵⁶ Article 248 § 2 CCivP.

It is accepted in the case law that it is permissible to oblige a third party to produce information based on data available to this third party.⁵⁷ A limitation on obtaining such evidence is provided by provisions on the protection of secrecy, for instance, on telecommunications secrecy. Therefore, in practice, it is assumed that a civil court may request a third party to provide electronic evidence, such as telecommunications data held by an OSP, only in situations where data concerning a party to the proceedings is involved and only with the party's consent.⁵⁸ In this respect, the President of the OCCP could possibly obtain electronic evidence for the purposes of proceedings resulting in the imposition of an administrative fine.

Furthermore, Article 50 of the CCPL stipulates a general obligation to provide all necessary information upon the President of the OCCP's request. This obligation applies to a wide range of entities, including entrepreneurs, natural persons, and legal persons that are not entrepreneurs, as well as other organisational units that are not legal persons but to which separate regulations grant legal capacity. This obligation applies to every entrepreneur, not just the one under investigation.⁵⁹ A request for information made by the President of the OCCP under Article 50 of the CCPL is binding for the requested person or entity. Refusal to provide the requested information, as well as providing false or misleading information (also unintentionally), are subject to a financial penalty.⁶⁰ Information or documents provided by a natural person may not be used to the detriment of that person or their relatives in proceedings conducted by the President of the OCCP for the imposition of a financial penalty.⁶¹

Article 50 of the CCPL does not specify what documents may be requested by the President of the OCCP, nor does it include electronic data in general. The lack of any further specification could indicate a broad understanding of this notion and allow the President of OCCP to request electronic evidence. Conversely, Article 51 CCPL, which concerns documentary evidence in proceedings before the President of the OCCP, refers to traditional documents and doesn't include electronic ones. However,

⁵⁷ Article 309 CCivP. See decision of the Supreme Court of 3.04.1974, II CZ 39/74, OSNC 1975, no. 6, item 93; decision of the Supreme Court of 30 June 2022, I CSK 1409/22, *Orzecznictwo Sądów Polskich* 2023, no. 10, item 76; cf. K. Bukalska, 'Podstawa prawna zobowiązania strony bądź osoby trzeciej do sporządzenia i przedstawienia informacji przed sądem. Glosa do postanowienia Sądu Najwyższego z dnia 30 czerwca 2022 r.', *Orzecznictwo Sądów Polskich*, 2023, no. 10, pp. 10-14.

⁵⁸ See M. Janik, 'Kwalifikacja dowodowa danych objętych tajemnicą telekomunikacyjną w postępowaniu cywilnym', *Monitor Prawniczy*, 2015, no. 3.

⁵⁹ See judgment of the Court of Appeal Warsaw of 1.03.2012, VI ACa 1033/11, LEX No. 1642375; judgment of the Court of Appeal Warsaw of 17.05.2016, VI ACa 630/15, LEX No. 2079176.

⁶⁰ Article 106 sec. 2 p. 2 CCPL.

⁶¹ Article 50 sec. 1 and 5 CCPL.

the literature indicates that, by applying the provisions of the CCivP, electronic evidence may also be used in proceedings before the President of the OCCP.⁶² The President of the OCCP may obtain them based on their voluntary surrender by investigated persons or through the President of the OCCP's investigatory powers, such as seizure and search.⁶³

During proceedings before the President of the OCCP, the investigator may request, *inter alia*, access to documents related to the subject of the inspection, correspondence sent by email, computer data carriers, other devices containing computer data, or computer systems if they may constitute evidence in the ongoing case.⁶⁴

The President of the OCCP may also issue a decision on the seizure of, *inter alia*, documents or correspondence, such as email, data carriers and devices containing data or systems, as well as other objects that may constitute evidence, for the time necessary to carry out the inspection, however, not longer than 7 days. In cases of competition-restricting practices, during investigations and antimonopoly proceedings, to find and obtain information from, *inter alia*, all kinds of documents, including data carriers, devices and systems, the President of the OCCP may conduct a search of the corporation's premises if there are reasonable grounds to believe that the said information or items are located there.⁶⁵

The inspection may be conducted with respect to a wide range of entities, as the only condition is that the controlled entity has the status of an entrepreneur. The scope of entities against which evidence may be seized is also not further specified in the CCPL. However, as seizure is possible within the framework of an inspection conducted by the President of the OCCP, so seizure may be made at any entrepreneur against whom the inspection is conducted. Generally, such an inspection is conducted in cases where an entrepreneur is suspected of violating competition protection regulations. However, it is also possible to conduct an inspection at entities that will not have the status of a party, for instance, a business partner of the corporation suspected of infringing the competition rules.⁶⁶ However, due to the

⁶² J. Krüger, in: A. Stawicki, E. Stawicki (eds.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, Warszawa, Poland, Wolters Kluwer Polska, 2016, p. 881; C. Banasiński, E. Piontek (eds.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, Warszawa, Poland, Lexis Nexis, 2009, thesis no. 11 to Art. 51.

⁶³ See C. Banasinski, E. Piontek (n. 68), thesis no. 11 to Art. 51.

⁶⁴ Article 105b sec. 1 and 2 CCPL.

⁶⁵ Article 105n CCPL.

⁶⁶ See B. Turno, in: A. Stawicki, E. Stawicki (n. 68), pp. 1230-1231; W. Jasiński, 'Gwarancyjność przepisów regulujących przeszukiwanie w sprawach ochrony konkurencji i konsumentów', p. 186, in: W. Jasiński (ed.), *Standardy rzetelności postępowania w sprawach z ochrony konkurencji i konsumentów. Między prawem administracyjnym a prawem karnym*, Warszawa, Poland, Wolters Kluwer Polska, 2016.

requirement of proportionality, a search at a third-party entity may be justified exceptionally if the evidence in question cannot be obtained otherwise.⁶⁷ Within this narrow scope, the President of the OCCP is therefore entitled to obtain electronic evidence from third parties through inspection and searches, as long as these documents or data may constitute evidence. The entity in possession of these documents or data is obliged to make them available to the inspector. Seizure is possible to prevent the content from being altered or destroyed. Following the seizure, the seized items are inspected, and a report is drafted. Generally, evidence obtained during an inspection may be used in the procedure for imposing a fine.

Persons whose rights have been violated may lodge a complaint against the decision to seize objects in court; however, lodging a complaint does not suspend the execution of the seizure decision. On the other hand, the President of the OCCP's decision regarding the inspection itself is not subject to appeal.⁶⁸

Searches can also be conducted in antitrust proceedings.⁶⁹ In a situation where there are reasonable grounds to believe that there are objects, files, books, documents and computer data carriers, stored in a apartment or in any other premises, property or means of transport, which may be relevant to establish facts related to the proceedings, the President of the OCCP may conduct a search to obtain information which may constitute evidence. Electronic evidence may therefore also be obtained under this procedure. A search on this basis may be performed at the premises of any entity, including a natural person. It requires the consent of the Court of Competition and Consumer Protection (*Sąd ochrony konkurencji i konsumentów*), granted at the request of the President of the OCCP. The President may request such authorisation only if there is a justified suspicion of a serious violation of the CCPL, in particular if evidence could be destroyed. The President of the OCCP may request that the police assist in these searches. To the extent not regulated in the CCPL, the provisions of the Code of Criminal Proceedings (CCP)⁷⁰ shall apply accordingly.

The person by whom the search is carried out has the right to appeal to the courts against the Court of Competition and Consumer Protection's decision to consent to the search.⁷¹ In the case of a search at a corporation's premises under Article 105n of the CCPL, both the corporation and the

⁶⁷ W. Jasiński (n. 72), pp. 186-187.

⁶⁸ See B. Turno (in:) A. Stawicki, E. Stawicki (n. 68), theses no. 1.1, 7 to Art. 105a.

⁶⁹ Article 91 CCPL.

⁷⁰ Law of 6.06.1997 – Code of Criminal Proceedings (*Kodeks postępowania karnego*), consolidated text: Journal of Laws 2025, item 46 as amended.

⁷¹ W. Jasiński (n. 72), pp. 195-196; M. Bernatt, in: T. Skoczny (ed.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, Warszawa, Poland, C.H. Beck, 2014, p. 1121.

persons whose rights have been violated during the search may also lodge a complaint to the Court of Competition and Consumer Protection, however, only against the search activities going beyond the subject matter of the search or other search activities undertaken in violation of the law. This is the subject of criticism, as it is not possible in this procedure to question the premises justifying the mere application of the search.⁷² In contrast, the scope of review of a search conducted under Article 91 of the CCPL is not limited.

3.1.5. GDPR enforcement

The provisions of the PDPL do not provide for any specific power to obtain evidence, including electronic evidence, from third parties during the proceedings conducted by the President of the PDPO. Although the President of the PDPO may carry out investigations on the compliance with the provisions on the protection of personal data, and the results of such proceedings may result in the initiation of proceedings for the infringement of these provisions, evidence may only be obtained from the supervised and investigated entity,⁷³ and only its employees may be questioned.⁷⁴ The CAP applies in this respect.

In practice, during PDPO's investigations, electronic evidence is sometimes obtained from the supervised entities themselves; however, this is typically in the form of hard copies. The PDPO does not receive electronic evidence from third parties. It has been pointed out that the Office is currently not even ready, from an organisational and technical point of view, to obtain such evidence. Furthermore, representatives of the PDPO perceive the need to regulate the collection of electronic evidence in the course of proceedings conducted by data protection authorities, especially given Regulation 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders applies to computer-related offences. These offences are often related to breaches of personal data protection.

4. TRANSFER OF DATA BETWEEN PROCEEDINGS

4.1. Transfers of data between national proceedings

In the current legal system, there are no specific provisions concerning the transfer of evidence collected in proceedings conducted by certain public administration authority to other administrative proceedings. Under the CAP, as a rule, evidence may be anything that contributes to clarifying the case and

⁷² W. Jasiński (n. 72), pp. 196-197.

⁷³ Article 84 PDPL.

⁷⁴ Article 86 PDPL.

is not contrary to law.⁷⁵ This position is accepted in case law.⁷⁶ The legal basis for using evidence collected in other administrative proceedings can also be sought in Article 7b CAP, which regulates the principle of cooperation of public administrative bodies. However, this provision has a character of a general rule, and a refusal to cooperate is not sanctioned in any way.

In administrative proceedings, it is also possible to use evidence gathered in other proceedings, including proceedings conducted by courts, prosecutors, the Police or other law enforcement authorities. This applies both to evidence gathered during criminal proceedings, including investigations into fiscal offences and fiscal contraventions.⁷⁷ The CAP does not contain any specific provision in that respect, which means that the basis for the use of evidence collected in proceedings conducted by the entities mentioned above will be Article 75 § 1 of the CAP. In the case law, the recognition of materials collected by other entities as evidence in administrative proceedings requires the fulfilment of two conditions: 1) they must be obtained per the law, and 2) a party must have the right to get acquainted with them and express their opinion on this evidence.⁷⁸ Nor does the CAP regulate the question of being bound by the content of this evidence. Therefore, it should be assumed that the administrative body is obliged to assess this evidence like any other evidence in the proceedings, under the general rules.⁷⁹ A court judgment is deemed as an official document⁸⁰, thus benefits from the presumptions of authenticity and truthfulness that are attributed to such evidence.⁸¹ Accordingly, factual findings made in criminal proceedings (e.g. relating to tax offences) based on the evidence gathered therein may be transferred via the judgment and its written reasons into the administrative proceedings.

Furthermore, the Code of Criminal Proceedings does not contain any general rule concerning the collection and use of evidence gathered in other proceedings, including administrative ones. However, the provisions of Articles 391 § 1 and 392 § 1 CCP allow, in situations indicated therein, the reading out of testimony given by a witness in non-criminal proceedings, provided that it is “provided for by law”. It follows the admissibility of the

⁷⁵ Article 75 § 1 CAP.

⁷⁶ Judgment of the Supreme Administrative Court of 27.02.2020, II GSK 3868/17, LEX No. 3031021.

⁷⁷ Judgment of the Voivodship Administrative Court Kielce of 19.12.2019, I SA/Ke 378/19, LEX No. 2763778; A. Mariański, ‘Swobodna czy dowolna ocena dowodów - teoria a praktyka’ *Przegląd Podatkowy*, 2008, no. 8, thesis no. 3.

⁷⁸ Order of the Supreme Administrative Court of 1.10.2018, I FPS 2/18, LEX No. 2592906.

⁷⁹ Order of the Supreme Administrative Court of 1.10.2018, I FPS 2/18, LEX No. 2592906.

⁷⁹ Article 77 § 1 CAP; Article 80 CAP and Article 81 CAP.

⁸⁰ Judgment of the Voivodship Administrative Court Łódź of 22.07.2022, III SA/Łd 419/20, LEX nr 3050144.

⁸¹ Article 76 CAP; R. Kędziora, *Ogólne postępowanie administracyjne*, Warszawa, Poland, C.H. Beck, 2019, p. 248.

use in criminal proceedings of minutes of testimony given in administrative proceedings.⁸² It follows also from Article 393 § 1 CCP the admissibility of the reading out in criminal proceedings of expert opinions and official documents submitted in the proceedings provided for by the law, which also means expert opinions and official documents obtained in administrative proceedings. Expert opinions from administrative proceedings may also refer to electronic evidence obtained in these proceedings.

The provision of Article 393 § 3 CCP allows the use as evidence in criminal proceedings of any private documents created outside criminal proceedings, without requiring that these documents come directly from a ‘private’ source. *Lege non distinguente* private documents may also be obtained ‘indirectly’ – through previous administrative proceedings. Private documents based on Article 393 § 3 CCP should also be understood as recordings and electronic evidence (arg. ex Art. 393a CCP).

In principle, it is permissible to use evidence obtained in administrative proceedings in criminal proceedings. The CCP does not impose any specific restrictions in that respect. This evidence is subject to evaluation based on general principles.

Specific provisions on transfers are provided for antitrust proceedings. Information obtained in the course of such proceedings may not be used in other proceedings conducted under separate provisions.⁸³ However, this does not apply, *inter alia*, to criminal proceedings concerning the offences prosecuted *ex officio* and fiscal offences.⁸⁴ This means that evidence from proceedings conducted by the President of the OCCP may be transferred for the purposes of criminal proceedings without restrictions. Furthermore, evidence of an opinion drawn up at the request of a public authority may be admitted in other proceedings provided for by law.⁸⁵ Thus, in a situation where an opinion has been drawn up in criminal proceedings, the subject of which is the analysis of computer data, it may also be used in proceedings before the President of the OCCP. In this indirect manner, electronic evidence obtained in criminal proceedings may be transferred to proceedings before the President of the OCCP.

Regarding transfers of evidence between the proceedings conducted by the FSC and criminal proceedings, Article 17ca LFMS provides for the possibility to exchange information and documents between the Chairman of the FSC and, *inter alia*, the Head of the Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego*), the Head of the Central Anti-Corruption

⁸² See *inter alia* D. Świecki (ed.), *Kodeks postępowania karnego. Komentarz*, Warszawa, Poland, Wolters Kluwer Polska, 7th ed., 2024, vol. 1, p. 1489.

⁸³ Article 73 sec. 1 CCPL

⁸⁴ Article 73 sec. 2 CCPL.

⁸⁵ Article 278 sec. 1 CCivP.

Bureau (*Centralne Biuro Antykorupcyjne*), the Head of the National Fiscal Administration (*Krajowa Administracja Skarbowa*), the Chief of the Police, the Chief of the Border Guard (*Straż Graniczna*), the Prosecutor General (*Prokurator Generalny*) and the National Public Prosecutor (*Prokurator Krajowy*), meaning, authorities authorised to conduct investigations and prosecutions in cases of criminal, including fiscal, offences. The transfer of documents can be bi-directional. The provision generally refers to information and documents, thus including documents in electronic form and data. The question of the origin of these documents is not specified; thus, they might have been obtained not only from entities participating in the proceedings but also from third parties. The LFMS stipulates that the transfer takes place “to the extent necessary for the performance of the statutory tasks” of the receiving authorities, and in the opposite direction, “to the extent necessary for the performance of the statutory tasks of the FSC”. The mutual exchange of information allows, among other things, the sharing of knowledge on identified undesirable phenomena in the financial market and the *modus operandi* used in committing illegal acts. Information sharing aims to better understand illegal behaviours and analyse them efficiently and consistently, thereby avoiding duplication or hindrance of actions. This enables the authorities to obtain information on the actions taken in relation to the individual acts of interest, thereby avoiding duplication of effort or action by a specific authority that could hinder the implementation of the adopted action plan by another authority.⁸⁶

The Article 17ca LFMS is of a very general nature. It mentions generally documents and information. It must therefore be assumed that these may also be documents in electronic form and electronic data. The origin of these documents is not specified, which may indicate that they may also be documents obtained not only from entities participating in the proceedings, but also from third parties.

4.2. Transfers of data between foreign and national proceedings

Polish law lacks a general regulation on the transfer of evidence from foreign administrative or criminal proceedings to domestic administrative proceedings. Due to the hierarchical system of sources of law, priority should be given to international agreements that concern specific areas of law. In the absence of international provisions, Article 75 § 1 CAP provides for an open catalogue of evidence in administrative proceedings (see Section 4.3). Thus, if evidence from foreign administrative or criminal proceedings is relevant to the decision in domestic administrative proceedings, it should be admitted.

⁸⁶ See K. Schulz, *Ustawa o nadzorze finansowym. Komentarz*, LEX/el. 2024, commentary to Art. 17ca.

Furthermore, the CCP does not contain any specific provision on the transfer of evidence from foreign administrative proceedings to domestic criminal proceedings. In principle, it is admissible to use the results of evidentiary acts carried out by “courts or prosecutors of foreign countries or authorities acting under their supervision”.⁸⁷ Therefore, the results of evidentiary acts carried out by administrative authorities of a foreign state are not admissible in Polish criminal proceedings.

4.3. Admissibility of data collected from online service providers as evidence

The admissibility of electronic evidence results from the principle of an open catalogue of means of evidence and the definition of evidence adopted in Article 75 § 1 CAP. According to the wording of this provision: “Anything that may contribute to the clarification of the case and is not contrary to the law should be admitted as evidence. In particular, evidence may be documents, witness statements, expert opinions and inspection”. Thus, evidence in administrative proceedings may be any medium of information regardless of the technical means of recording, provided that the requirement of Article 75 § 1 sentence 1 in fine CAP is observed, meaning, its collection is not irregular by law.⁸⁸

There are also no specific provisions on electronic evidence in the Tax Ordinance. Their admissibility results, as in administrative proceedings, from the principle of an open catalogue of means of evidence and the definition of evidence. According to Article 180 § 1 of the Tax Ordinance, everything that may contribute to clarifying the case and is not contrary to law should be admitted as evidence. This regulation is supplemented by Article 181 of the Tax Ordinance, containing an exemplary catalogue of evidence in tax proceedings. It indicates that evidence in tax proceedings may be, in particular, tax books, declarations submitted by a party, testimonies of witnesses, opinions of experts, materials and information collected as a result of inspection, tax information and other documents collected in the course of analytical activities of the National Fiscal Administration, checking activities, tax control or customs and fiscal control, as well as materials collected in the course of criminal proceedings or proceedings in cases of fiscal offences or fiscal contraventions.

Although the provisions of the CCivP do not explicitly mention electronic evidence, it is accepted in case law that such evidence, such as emails or text messages, is in principle admissible and may be used in civil

⁸⁷ Article 587 CCP.

⁸⁸ R. Suwaj (no. 46), pp. 121-122.

proceedings,⁸⁹ due to the principle of an open catalogue of evidence in civil proceedings.⁹⁰ Based on this catalogue, it is possible to admit any evidence not explicitly indicated in the CCivP, including electronic evidence.

5. CONCLUSION

Polish regulations on administrative proceedings for the imposition of administrative fines provide for the possibility of obtaining evidence from third parties to a minimal extent. There is no legal basis for obtaining electronic evidence from OSPs. The legal frameworks governing requests for data from OSPs vary across different areas of enforcement in Poland. In customs and VAT proceedings, authorities have limited means to compel third parties to provide evidence, with some exceptions for financial institutions in ongoing tax cases. In banking and financial market enforcement, investigations by the Financial Supervision Commission are limited to the controlled entities and do not extend to third parties. In competition law, broader powers exist: the President of the OCCP can compel the disclosure of information and conduct searches and seizures, including electronic evidence, even from third parties, under strict conditions. However, procedural safeguards apply. In GDPR enforcement, the data protection authority lacks explicit powers to collect electronic evidence from third parties. It is currently not equipped to do so, highlighting a regulatory and operational gap. Also, the issue of transfer of evidence between administrative and criminal proceedings has not been regulated in any way.

⁸⁹ See, e.g., judgment of the Court of Appeal Gdańsk of 24.05.2018, V ACa 392/17, LEX No. 2692147; judgment of the Court of Appeal Kraków of 20.12.2016, I ACa 960/16, LEX No. 2692147.

⁹⁰ Article 309 CCivP.

13. GATHERING ELECTRONIC EVIDENCE IN ADMINISTRATIVE PROCEEDINGS: COMPARATIVE ANALYSIS OF LAW AND PRACTICE

S. TOSZA, S. LANNIER and F. JUNG

1. INTRODUCTION

The ELEVADMIN project was launched to address a critical and underexplored issue: the gathering of electronic evidence from Online Service Providers (OSPs) in administrative punitive investigations. Although electronic evidence has been widely examined in the context of criminal investigations, its role in administrative enforcement, especially within EU institutions and Member States, remains insufficiently studied. This research project seeks to fill that gap by analysing the legal foundations, operational procedures, and institutional capacities for administrative authorities to obtain electronic evidence from OSPs. This chapter undertakes a detailed comparative analysis across nine EU Member States, Belgium, Finland, France, Germany, Ireland, Italy, Luxembourg, the Netherlands, and Poland. It focuses on five key domains of administrative punitive enforcement: customs, Value Added Tax (VAT), competition law, data protection, and financial market supervision. These areas were selected for their relevance to the protection of the EU's financial interests and their varying degrees of overlap between administrative and criminal enforcement mechanisms. The findings reveal a fragmented and evolving legal landscape. This chapter identifies a mosaic of legal provisions, with considerable variation in the scope of authority, types of data accessible, procedural safeguards, and enforcement tools. Crucially, existing frameworks tend to receive limited procedural guarantees. Moreover, the rules governing the admissibility and transfer of electronic evidence, especially between administrative and criminal proceedings, are inconsistent and largely undeveloped, relying primarily on the general principle of free evaluation of evidence.

Despite the growing digitalisation of society, administrative authorities across studied jurisdictions have shown limited interest in gathering electronic evidence from third parties, particularly OSPs. This limited engagement with OSPs may not solely reflect institutional inertia or lack of

awareness. Rather, it may be rooted in deeper structural issues, including the absence of clear or suitable legal frameworks enabling such requests, or the perceived irrelevance of OSP-held data in certain enforcement contexts. Depending on the sector, the nature of the investigation, and the types of data typically required, administrative authorities may find that traditional sources, such as records held by the investigated entity, remain more accessible or probative. In some cases, the legal basis for requesting data from third parties is either too vague or narrowly defined, discouraging authorities from pursuing digital evidence beyond conventional means. This chapter explores how these legal and practical constraints shape the appetite for electronic evidence across jurisdictions and sectors.

Historically, evidence collection has focused on physical or on-site methods, as seen in the Netherlands where the 1990s General Administrative Law Act.¹ Similarly, in France, authorities supervising financial institutions have found little utility in sourcing information from third parties, preferring direct engagement with supervised entities.² Finland mirrors this trend, with VAT enforcement occasionally employing broad interpretations for evidence gathering but lacking established practices or case law concerning third-party data collection.³ Finnish competition authorities primarily rely on on-site inspections, given the legal obligation for suspected entities to cooperate.⁴ Belgium and Luxembourg also lean towards on-site collection, with Luxembourg's VAT authorities seldomly requesting data from others than taxpayers⁵ and Belgium's data protection authority collecting most evidence on-site.⁶

However, this approach is beginning to evolve. In the Netherlands, administrative bodies are seeking powers better suited to technological advancements, though practical use remains rare.⁷ Finland has seen isolated instances where the data protection authority accessed subscriber data from telecom operators,⁸ and there is increasing demand for access to traffic data by authorities supervising financial institutions.⁹ France's legislative

¹ A. De Vries et al., 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in the Netherlands', in this book, p. 342.

² M. Lassalle, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in France', in this book, p. 180.

³ J. Riekkinen, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in Finland', in this book, p. 142.

⁴ *Ibid.* pp. 149, 152-153, 156.

⁵ S. Lannier, S. Tosza, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in Luxembourg', in this book, p. 303.

⁶ V. Franssen, M. Vandormael, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in Belgium', in this book, pp. 101-103.

⁷ De Vries et al., (n. 1), pp. 343, 354.

⁸ Riekkinen, (n. 3), p. 157.

⁹ *Ibid.* p. 145.

framework is gradually adapting under EU influence to craft new powers to gather telecommunication data in administrative proceedings,¹⁰ and Belgium's competition authority has recently gained the ability to collect metadata.¹¹ Similarly, Ireland's legislative framework has undergone significant evolution influenced by developments in European Union law, positioning the country as a central hub for the headquarters of various international OSPs.¹² These entities play a crucial role in the collection of digital evidence. However, a comprehensive general framework addressing this domain remains absent.¹³

In parallel, recent years have seen a growing trend of public-private partnerships in data collection and enforcement activities across various jurisdictions, particularly in areas such as competition law, financial oversight, and tax enforcement. In the Netherlands, authorities have engaged in cooperative ventures with private actors to combat serious organised crime, leveraging external expertise and data sources.¹⁴ Similarly, in Finland, competition law has been interpreted to allow the Finnish Competition and Consumer Authority (FCCA) direct access to public tender data through a private service provider, while customs authorities routinely obtain information from both public and private databases.¹⁵ Belgium has also embraced private sector collaboration in competition law enforcement, notably in the collection, processing, and analysis of electronic evidence obtained during on-site inspections.¹⁶ In Italy, tax authorities have gone even further by utilising social media and private digital platforms to detect tax evasion. Through partnerships with private companies, Italian authorities have cross-referenced online content—such as influencer marketing activities and adult platform earnings—with declared incomes, uncovering discrepancies.¹⁷

These developments suggest a shifting landscape where administrative authorities are starting to recognise the potential and necessity of leveraging electronic evidence in enforcement activities. In the face of this shift, this chapter analyses the powers of administrative authorities in selected areas of enforcement to gather data from third parties.

¹⁰ Lassalle, (n. 2), pp. 172-173.

¹¹ Franssen, Vandormael, (n. 6) p. 101.

¹² N. Ni Loideain, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in Ireland', in this book, p. 245.

¹³ *Ibid.* p. 246.

¹⁴ De Vries et al., (n. 1), p. 368.

¹⁵ Riekkinen, (n. 3), p. 158.

¹⁶ Franssen, Vandormael, (n. 6), p. 102.

¹⁷ G. Lasagni, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in Italy', in this book, p. 280.

To guide the reader through this complex and evolving landscape, the chapter adopts a structure that mirrors the progression typically found in the national chapters of this volume. It begins by examining the general structure of administrative punitive enforcement, which frames how investigative powers are allocated and exercised. This sets the foundation for the subsequent analysis of powers to gather data from third parties, starting with ‘specific powers’ granted to administrative authorities to request electronic evidence specifically from OSPs, a growing and often contentious domain. This is followed by a discussion of ‘general powers’ to request information from any third parties more broadly, which are often more ambiguously framed yet equally relevant in practice. The chapter then turns to the conditions for requesting such data and the types of data that may be accessed, before exploring the transfer and enforcement mechanisms available when OSPs fail to comply. Finally, it addresses the legal safeguards available to both third parties, including OSPs, and investigated persons, as well as the admissibility and further use of data obtained in administrative proceedings.

2. THE STRUCTURE OF ADMINISTRATIVE PUNITIVE ENFORCEMENT

The structure of administrative punitive enforcement plays a crucial role in determining how regulatory authorities operate, the legal tools available to them, and the extent to which procedural safeguards are applied. As administrative sanctions increasingly serve functions traditionally reserved for criminal law, such as deterrence and punishment, many jurisdictions are grappling with the boundaries between supervisory, investigative, and punitive actions. This section examines the legal and institutional arrangements underpinning administrative enforcement across selected jurisdictions. It explores the classification of proceedings, the division of powers between administrative and criminal bodies, and the overarching legislative frameworks that shape how administrative authorities investigate and sanction regulatory breaches.

2.1. Criminal, supervisory and punitive administrative proceedings

Understanding the distinctions and overlaps between criminal, supervisory and punitive administrative proceedings is essential for analysing how different legal systems approach the enforcement of regulatory norms. While traditionally viewed as separate domains, many jurisdictions exhibit hybrid structures in which administrative authorities exercise powers with punitive or quasi-criminal effects. This sub-section explores how the studied legal orders define and organise these different proceedings, focusing on the allocation of investigative and enforcement powers, the interplay between

administrative and criminal mechanisms, and the general procedural safeguards triggered by punitive measures.

The distinction between criminal and administrative enforcement is fundamental to understanding how different jurisdictions approach regulatory compliance and sanctions. Criminal enforcement typically involves the prosecution of offences that are considered harmful to public order, leading to penalties such as imprisonment or criminal fines, and follows strict procedural safeguards. In contrast, administrative enforcement addresses regulatory breaches through sanctions like administrative fines or corrective measures, often with more flexible procedures. Germany clearly separates these two systems: criminal offences are subject to mandatory prosecution by criminal authorities, while regulatory offences fall under administrative enforcement guided by the principle of opportunity.¹⁸ The Netherlands and Italy, however, employ a dual enforcement system where authorities may choose between administrative or criminal proceedings based on the nature of the offence.¹⁹ Belgium blends these approaches, with enforcement mechanisms varying across sectors depending on specific legislation and practices.²⁰

Within administrative enforcement itself, there is also a distinction between supervision and investigation. Supervisory activities are preventive and aim to ensure compliance through monitoring and guidance, while investigative actions are reactive, focusing on detecting and addressing potential violations. Germany exemplifies this separation, with banking law and financial markets law assigning supervision and investigation to different departments within supervisory authorities.²¹ Conversely, the Netherlands, despite distinguishing between reparatory and punitive sanctions,²² grants administrative authorities identical powers for supervision and investigation.²³ Luxembourg,²⁴ Finland,²⁵ and Poland,²⁶ for the latter particularly regarding financial supervision, make no clear distinction between these functions, allowing authorities to seamlessly transition from supervision to investigation. This blurred line is particularly relevant when administrative bodies have dedicated criminal units—such as customs

¹⁸ P. Blume et al., ‘Gathering of Electronic Evidence in Administrative Punitive Proceedings in Germany’, in this book, p. 208

¹⁹ De Vries et al., (n. 1), p. 333; Lasagni, (n. 17), p. 267.

²⁰ Franssen, Vandormael, (n. 6), p. 87.

²¹ Blume et al., (n. 18), p. 229.

²² De Vries et al., (n. 1), p. 337.

²³ *Ibid.* p. 338.

²⁴ See *infra* Section 3.2.

²⁵ Riekkinen, (n. 3), p. 136.

²⁶ K. Kaszubowski, S. Steinborn, ‘Gathering of Electronic Evidence in Administrative Punitive Proceedings in Poland’, in this book, p. 379.

enforcement agencies in Belgium,²⁷ Finland,²⁸ France,²⁹ Germany,³⁰ Italy,³¹ Luxembourg,³² and Poland,³³ and tax administrations in Belgium,³⁴ Italy,³⁵ Germany,³⁶ the Netherlands³⁷ and Poland³⁸—which are enabled to apply criminal procedural rules when necessary. This blurred line is also sensitive when authorities receive discretionary power to impose either an administrative fine or to transfer the evidence towards criminal proceedings (see Section 4.1.1).³⁹ This structural variation across jurisdictions significantly influences how evidence is gathered and how enforcement measures are implemented.

Although administrative enforcement proceedings are formally classified as administrative in nature, there is a growing recognition that many of these proceedings qualify as ‘criminal in nature’ under the case law of the European Court of Human Rights (ECtHR).⁴⁰ This classification hinges on the severity and purpose of the sanctions imposed, which often mirror criminal penalties in their punitive intent and impact. In the Netherlands, legal literature widely acknowledges that administrative fines may be considered criminal in nature due to their punitive and deterrent functions.⁴¹ Similarly, in Finland, scholars recognise that punitive administrative proceedings must adhere to the same procedural safeguards and due process rights as criminal proceedings.⁴² This is particularly evident in sectors prone to economic misconduct, where administrative sanctions act as substitutes for criminal punishment.⁴³ Luxembourg also reflects this trend, with legal scholarship identifying sanctions imposed by financial sector⁴⁴ and data protection⁴⁵ authorities as criminal in nature. Belgium reflects a comparable trend, notably in competition law, where the Market Court, acknowledging the criminal

²⁷ Franssen, Vandormael, (n. 6), p. 85.

²⁸ Riekkinen, (n. 3), p. 127.

²⁹ Lassalle, (n. 2), p. 170.

³⁰ Blume et al., (n. 18), p. 202.

³¹ Lasagni, (n. 17), p. 268.

³² Lannier, Tosza, (n. 5), p. 194.

³³ Kaszubowski, Steinborn, (n. 26), p. 378.

³⁴ Franssen, Vandormael, (n. 6), p. 89.

³⁵ Lasagni, (n. 17), pp. 269-270.

³⁶ Blume et al., (n. 18), p. 202.

³⁷ De Vries et al., (n. 1), p. 334.

³⁸ Kaszubowski, Steinborn, (n. 26), p. 378.

³⁹ *Ibid.* p. 379.

⁴⁰ S. Tosza, S. Lannier, M. Siclari, ‘Bridging the Gap: Electronic Evidence in Administrative Investigations’, in this book, p. 1 ff.

⁴¹ De Vries et al., (n. 1), p. 338.

⁴² Riekkinen, (n. 3), p. 133.

⁴³ *Ibid.* p. 132.

⁴⁴ Lannier, Tosza, (n. 5), p. 296.

⁴⁵ *Ibid.* p. 297.

nature of administrative sanctions, provides full judicial oversight.⁴⁶ The Belgian Competition Authority has explicitly accepted that its sanctions carry a criminal character,⁴⁷ and in 2023, sanctions in the financial markets sector were officially recognised as criminal in nature under the European Convention on Human Rights (ECHR).⁴⁸ In Italy, the Italian Supreme Court and Constitutional Court have similarly recognised the criminal nature of sanctions imposed by the banking, financial markets and competition supervisors.⁴⁹ The latter authority may explicitly impose ‘punitive sanctions’, although such a category is not defined.⁵⁰ Comparably, in Ireland, following the *Zalewski* judgment, administrative entities may perform acts that are criminal in nature but must respect the law and principles of fair procedure. This includes investigative powers that may affect fundamental rights, for example regarding witnesses, as highlighted in the Irish case law referring to the ECtHR case law.⁵¹ Germany differentiates between criminal and regulatory offences based on the sanction’s nature, with the Federal Constitutional Court distinguishing criminal offences as carrying ‘socio-ethical or dishonourable unworthiness’, whereas regulatory fines are viewed as ‘disobedience to the administration’.⁵² Nonetheless, Germany’s Act on International Mutual Assistance in Criminal Matters extends to regulatory offences, underscoring their quasi-criminal character.⁵³ This evolving perspective across jurisdictions necessitates the application of enhanced procedural safeguards—to ensure compliance with ECHR standards and to protect individuals from disproportionate state action in administrative enforcement proceedings.

2.2. Legislative overview of administrative proceedings

The legislative foundations of administrative enforcement differ markedly across jurisdictions, reflecting varying legal traditions, institutional structures, and approaches to administrative proceedings. While some countries rely on comprehensive and codified administrative procedure acts, others primarily regulate administrative proceedings through fragmented, sector-specific statutes. These divergences influence not only the coherence and accessibility of the legal framework but also the scope of investigative powers, the availability of procedural safeguards, and the consistency of

⁴⁶ Franssen, Vandormael, (n. 6), p. 88.

⁴⁷ *Ibid.*

⁴⁸ *Ibid.* p. 87.

⁴⁹ Lasagni, (n. 17), p. 284.

⁵⁰ *Ibid.* pp. 270-271.

⁵¹ Ni Loideain, (n. 12), p. 251.

⁵² Blume et al., (n. 18), pp. 205-207.

⁵³ *Ibid.* p. 240.

enforcement practices. This comparative overview of the legislative regimes governing administrative proceedings also explores the role of general principles of administrative law, and the implications for gathering electronic evidence from third parties.

The legislative structure governing administrative enforcement and investigation powers across the studied countries reveals a contrast between comprehensive general frameworks and fragmented sector-specific regulations. Germany exemplifies a more structured approach through the Act on Regulatory Offences, which governs administrative sanctions but refers to the Criminal Procedure Code for procedural matters, with necessary adaptations and explicit exclusions—for instance, limiting criminal investigative powers to a defined list of offences.⁵⁴ Finland adopts a similar general framework with its Administrative Procedure Act, applicable to all administrative matters, including investigations and punitive sanctions.⁵⁵ The Netherlands relies on the General Administrative Law Act of 1994, which standardises administrative procedures but notably excludes customs and tax matters, leaving these areas governed by separate legal frameworks.⁵⁶ Luxembourg operates under the 1978 Law on Non-Contentious Administrative Procedure and the 1979 Grand-Ducal Regulation, although their applicability to VAT enforcement remains ambiguous and these frameworks remain barely detailed.⁵⁷ Similarly, Italy⁵⁸ and Poland⁵⁹ rely on general administrative law on proceedings, which contains only general minimum rules. However, in all cases, these frameworks must be supplemented by sector-specific legislation detailing sanctions and procedural rules for particular sectors.

In contrast, France,⁶⁰ Belgium,⁶¹ Italy⁶² and Luxembourg lean heavily on sector-specific legislation, resulting in a fragmented and sometimes inconsistent legal framework. This is particularly evident in the financial sector, where Luxembourg has an array of over 15 distinct laws, each outlining supervisory powers with varying levels of detail and coherence.⁶³ Similar diversity can be found in the banking sector in Italy.⁶⁴ In Ireland, the fragmented legal framework results from the absence of codification in Irish

⁵⁴ *Ibid.* pp. 209-212.

⁵⁵ Riekkinen, (n. 3), p. 134.

⁵⁶ De Vries et al., (n. 1), p. 337.

⁵⁷ Lannier, Tosza, (n. 5), p. 301.

⁵⁸ Lasagni, (n. 17), p. 285.

⁵⁹ Kaszubowski, Steinborn, (n. 26), p. 380.

⁶⁰ Lassalle, (n. 2), p. 172.

⁶¹ Franssen, Vandormael, (n. 6), p. 87.

⁶² Lasagni, (n. 17), p. 267.

⁶³ Lannier, Tosza, (n. 5), p. 305.

⁶⁴ Lasagni, (n. 17), p. 268.

law.⁶⁵ However, the Irish Constitution establishes a foundation for investigating and enforcement powers in both administrative and criminal proceedings.⁶⁶ Recently, there has been a shift from a rigid judicial ‘centralism’ to a sector specific distribution of powers to administrative bodies.⁶⁷

Generally, administrative punitive proceedings across the surveyed jurisdictions are governed by foundational legal principles designed to ensure fairness, legality, and the protection of fundamental rights. These principles, though not always codified, significantly influence administrative practices. Most jurisdictions refer to the principle of proportionality in administrative proceedings (NL, LU, GE, FI, IT, PL). Additionally, in the Netherlands, the principles of good administration, competence of the supervisory authority, and observance of fundamental rights guide proceedings.⁶⁸ Also, subsidiarity requires authorities to first seek information directly from the concerned party.⁶⁹ These general principles can be explicitly embedded in sectorial legislations, such as in Belgium, where the data protection authority must justify data requests by demonstrating proportionality and subsidiarity.⁷⁰ Luxembourg mandates that administrative authorities exercise decision-making powers impartially and act within a reasonable timeframe, and the country enshrines rights of defence and the adversarial principle under its Law governing non-contentious administrative procedures.⁷¹ Germany integrates core criminal law principles such as the principle of legality, *lex mitior*, *in dubio pro reo*, the right to be heard, and the right to remain silent.⁷² In Finland, constitutional guarantees underpin the legality of investigatory powers, necessitating precision in legal provisions and ensuring the right to an effective remedy, a fair trial, and good administration. Some general principles are differently protected under statutory law. Finnish law emphasises equal treatment, impartiality, and the right to be heard, requiring precise and timely communication in administrative procedures.⁷³ Similarly, Irish case law integrates the impartiality and independence of decision-makers as fundamental components of the good administration of justice.⁷⁴

⁶⁵ Ni Loideain, (n. 12), pp. 247, 252.

⁶⁶ *Ibid.* pp. 247-248.

⁶⁷ Franssen, Vandormael, (n. 6), p. 87.

⁶⁸ De Vries et al., (n. 1), p. 339.

⁶⁹ *Ibid.* p. 341.

⁷⁰ Franssen, Vandormael, (n. 6), p. 102.

⁷¹ Lannier, Tosza, (n. 5), p. 300.

⁷² Blume et al., (n. 18), p. 208.

⁷³ Riekkinen, (n. 3), pp. 133-134.

⁷⁴ Ni Loideain, (n. 12), p. 250.

3. THE CONTENT OF ADMINISTRATIVE INVESTIGATION POWERS TOWARDS OSPs

The growing reliance on OSPs as key data holders in administrative investigations has prompted a gradual expansion of investigatory powers across jurisdictions. This section provides a comparative overview of how these powers are structured and exercised, revealing a fragmented and often ambiguous legal landscape. While some authorities benefit from clearly defined, sector-specific powers to request data from OSPs ('specific powers'), others rely on broadly framed general powers whose applicability to OSPs is not always explicit ('general powers'). The analysis shows that the scope of powers, the categories of data accessible, and the conditions for requesting information vary significantly, often depending on the area of enforcement. Moreover, the distinction between specific and general powers is not always clear-cut in practice, and the legal frameworks frequently lack coherence or harmonisation. This section highlights the operational and normative challenges that arise when administrative authorities seek to access electronic evidence from actors who are not the primary subjects of investigation but are essential to its success.

3.1. Specific administrative powers to gather data

Specifically, some administrative authorities are granted powers, in some jurisdictions, to request data from OSPs. This section focuses on the categories of OSPs subject to such powers, the categories of data that may be accessed, and the legal and procedural conditions under which these powers may be exercised across jurisdictions. These powers are typically grounded in sector-specific legislation and are often shaped by EU law, though their scope and implementation vary significantly across the studied jurisdictions. The comparative analysis reveals that while some countries provide detailed and narrowly defined powers, clearly distinguishing between types of data and requiring strict conditions, others rely on broader or less clearly delimited frameworks. The categories of OSPs subject to these powers, the types of data that may be accessed and the conditions under which access is granted differ widely, with some authorities enjoying expansive reach and others facing legal or constitutional constraints. Overall, the section highlights a fragmented legal landscape which does not yet match the growing reliance on electronic evidence.

3.1.1. Categories of OSPs as addressees to specific powers to request data

In most countries (except in the Netherlands), administrative authorities are entitled to request data from certain types of third parties, including from OSPs. To delimit the addressees of these requests, some countries use, as in Poland,⁷⁵ or refer to definitions under EU law, although the transposition of these definitions are not always fully harmonised. Indeed, countries retain a certain margin of appreciation in transposing EU texts defining categorising OSPs. Certain legal cultures heavily rely on references to other frameworks, while others retain sectorial definitions and categories. Indeed, administrative proceedings frameworks do not always refer to national frameworks on electronic communications, leading to the multiplication of categories of OSPs and questioning the legal coherence among legal frameworks. Therefore, as in criminal law, definitions and categories of OSPs remain diverse at EU level.⁷⁶

In Germany, all authorities can, under the general framework on regulatory offences investigation, specifically request subscriber data from providers of electronic communications service under the European Electronic Communications Code,⁷⁷ and from providers of digital services classified as Information Society services under the Information Society Services Directive.⁷⁸

Most of the specific powers to gather data stem from sectorial legislation, although OSPs categories remain diverse even within one jurisdiction. For instance, Belgium's competition authority, since January 2023, may access data from electronic communications operators active on the Belgian market.⁷⁹ Similarly, Belgium's data protection authority may request data from electronic communication network operators within Belgian territory,⁸⁰ which categories derive from EU law. Finally, Belgium's financial markets supervisor may request metadata and identification data from operators of telecommunications networks and providers of a telecommunications service.⁸¹

⁷⁵ Kaszubowski, Steinborn, (n. 26), p. 382.

⁷⁶ V. Franssen, S. Tosza, 'A Comparative Analysis of National Law and Practices - Unravelling Differences in View of EU-Wide Solutions', in: V. Franssen, S. Tosza (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Matters*, Cambridge University Press, 2025, pp. 423-454.

⁷⁷ Article 2(4) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11.12.2018 establishing the European Electronic Communications Code.

⁷⁸ Blume et al., (n. 18), pp. 216-217. Article 1.1(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 09.09.2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

⁷⁹ Franssen, Vandormael, (n. 6), p. 102.

⁸⁰ *Ibid.*

⁸¹ *Ibid.* p. 92.

France grants similar powers to gather telecommunication metadata to various authorities, including customs, VAT, financial market and competition supervisors. These powers cover electronic communications operators—defined as any entity operating a public electronic communications network or providing related services—and service providers offering online public communication services or hosting user-generated content.⁸² In Ireland, the term OSP is broadly defined, encompassing a wide range of internet services, including *inter alia* webmail, messaging providers, hosting services, online marketplaces and search engines.⁸³

In other countries, specific administrative powers to gather data are limited to the financial institution sectors. In Luxembourg, authorities in the financial institution sectors may request data from providers of electronic communication services and operators of public communication networks. Although those categories retain the wording of EU texts, Luxembourg's framework does not include, as under EU law, internet access or interpersonal communication services among electronic communications services.⁸⁴ Additionally, while some authorities may request telecommunications data from any entity, it remains unclear whether the power to issue such requests concerns only the entities under investigation or extends to other supervised entities acting as third-party OSPs, particularly in the data protection sector.⁸⁵ In Italy, administrative authorities may specifically request data only in the context of market abuse investigations, where the competent administrative authority may issue requests simply to anyone, or in certain context only to providers of the traffic data.⁸⁶ In Germany, supervisors in the financial institution sectors may request traffic data from telecommunications operators,⁸⁷ as well as communication data from securities trading companies, data provision services, credit institutions, supervised entities, and financial institutions.⁸⁸ Therefore, the vocabulary used at the national level to define entities subject to data requests by administrative authorities shows varying degrees of alignment with EU definitions.

The vocabulary issues aside, specific powers are usually granted to competition, data and financial institutions supervisors, as a transposition of

⁸² Lassalle, (n. 2), p. 174.

⁸³ Ni Loideain, (n. 12), p. 245.

⁸⁴ Lannier, Tosza, (n. 5), pp. 301.

⁸⁵ *Ibid.* pp. 307-308.

⁸⁶ Lasagni, (n. 17), pp. 271-272.

⁸⁷ Blume et al., (n. 18), p. 207.

⁸⁸ *Ibid.* p. 229.

EU law, but these powers tend to extend the scope set for such powers under EU legislation, as they are created in other areas of enforcement.⁸⁹

3.1.2. Categories of data under specific powers

The types of data that administrative authorities may request under their national frameworks vary significantly, reflecting differing national approaches to balancing investigatory needs with data protection and privacy safeguards. Overall, while some countries provide detailed definitions of data categories (e.g., Germany), others adopt broader or less defined terms (e.g., France and Luxembourg). In countries granting some administrative authorities with specific powers to request data from OSPs, there are discrepancies in the scope of data that may be accessed at national level among areas of enforcement. Exclusions, especially regarding sensitive data such as dynamic IP addresses, are still little considered.

In France, administrative authorities may only request, under specific powers to gather data from OSPs, one category of data, namely, ‘telecommunication metadata’, which may be gathered from entities subject to data retention obligations. Yet, the law does not clearly define the scope of this data category.⁹⁰

Germany provides a detailed classification of data types. All authorities may request subscriber data—such as telephone numbers, names, addresses, dates of birth, device numbers, and contract details—, including voluntarily stored data like usernames, passwords, and PINs. However, this excludes login data related to end devices or separate storage devices.⁹¹ The financial institutions supervisors may request traffic data, which includes call and connection details (e.g., port identifiers, card numbers, timestamps, and data volumes)⁹² and communication data like call recordings and electronic messages, but access is limited to historical (past) data due to privacy protections.⁹³ In all cases, requests only regard stored, that is, past, data. Importantly, dynamic IP addresses are excluded due to constitutional protections of telecommunications secrecy and the ‘double door model’.⁹⁴

⁸⁹ Franssen, Vandormael, (n. 6), pp. 85, 87, see for instance, Article 69.2(d) of Directive 2014/65/EU of the European Parliament and of the Council of 15.05.2014 on markets in financial instruments; Article 98.1(d) of Directive 2009/65/EC of the European Parliament and of the Council of 13.07.2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities.

⁹⁰ Lassalle, (n. 2), p. 173.

⁹¹ Blume et al., (n. 18), p. 217-218.

⁹² *Ibid.* pp. 227-228.

⁹³ *Ibid.* p. 228.

⁹⁴ *Ibid.* p. 219.

Other countries rely on multiple or vague categories of data, allowing, in theory, to request disclosure of any kind of data. In Belgium, the competition authority may access traffic data, location data, and other electronic records from communications operators.⁹⁵ The Belgian financial markets and data protection authorities may obtain data identifying subscribers or habitual users of electronic communication services.⁹⁶ Additionally, the Belgian financial markets authority may request telecommunication calls data, such as the origin or destination of the telecommunication.⁹⁷ The data protection authority may request any data necessary to identify subscribers or regular users of devices. In Luxembourg, the financial institutions authorities may access traffic data from certain OSPs, defined as data processed for routing communications or billing purposes, and distinguished from location data.⁹⁸ Luxembourg also allows the collection by the same authorities, from anyone, of telephone recordings, electronic communications, records of data exchanges, and broader categories of ‘electronic records’.⁹⁹ In Italy, the financial supervisor may access recordings of telephone conversations, electronic communications, and data exchange or any type of personal data from anyone in the context of market abuse or from supervised entities and telecommunication operations in other areas of financial law, and traffic data from providers in both cases. However, addressees may invoke secrecy to refuse to provide data.

3.1.3. Conditions to request data from certain OSPs

The conditions under which administrative authorities may request data from OSPs reveal a complex interplay of legal safeguards, investigative thresholds, and procedural requirements. While the principle of necessity emerges as a common baseline, its interpretation and application vary widely, often, intersecting with other conditions such as proportionality, relevance, and the existence of a reasonable suspicion. In some legal systems, these conditions are cumulative and tightly regulated while in others, they are loosely defined or sector-specific, leaving room for discretion and legal uncertainty. This diverse landscape reflects varying balances between investigative needs and the protection of fundamental rights across national frameworks.

The conditions under which administrative authorities may request data from certain OSPs often reflect the severity of the offence and the necessity of the data. In France, telecommunication metadata access is strictly tied to

⁹⁵ Franssen, Vandormael, (n. 6), pp. 100-101.

⁹⁶ *Ibid.* p. 102.

⁹⁷ *Ibid.* p. 96.

⁹⁸ Lannier, Tosza, (n. 5), p. 301.

⁹⁹ *Ibid.* p. 308.

the nature of the offence: customs authorities may only request such data for enumerated serious offences such as intentional smuggling and customs fraud,¹⁰⁰ VAT authorities for aggravated administrative offences, e.g. underreporting,¹⁰¹ and the financial markets authority exclusively for market abuse investigations.¹⁰² In Italy, data may only be requested for investigations specifically relating to market abuse.¹⁰³ Differently, the French¹⁰⁴ and Italian¹⁰⁵ competition authorities may request such data generally to investigate any anti-competitive practices. Similarly, in Germany, requests for subscriber data to digital service providers are limited to regulatory offences where fines exceed 15.000 euros, encompassing such areas as VAT violations, banking, financial markets, and GDPR breaches.¹⁰⁶

One of the requirements to obtain data is the need to demonstrate the necessity of the data for the investigation in question. In Germany, requests for subscriber data must be based on an initial suspicion and must be necessary to establish facts or locate a suspect.¹⁰⁷ The access to traffic data by the financial institutions supervisors requires a facts-based suspicion of a breach and proof that the data is necessary for investigation.¹⁰⁸ In Italy, the data must as well be necessary for the investigation of market violations.¹⁰⁹ In Luxembourg, financial institutions authorities must show a reasonable suspicion of an infringement and that the requested records are likely to aid in establishing the truth.¹¹⁰ In Ireland, any person may be asked by the VAT authority to provide reasonable assistance when exercising its powers.¹¹¹ A similar principle can be found under Polish law, as the data must be relevant for the ongoing case.¹¹² Additionally, in Poland, although requesting telecommunications is theoretically possible, telecommunications secrecy would require that parties to the communications should consent to its disclosure by the requested OSP.¹¹³ The requirement of judicial authorisation or of approval by an independent body to access data varies across jurisdictions, reflecting different approaches to safeguarding privacy and ensuring proportionality. While the lack of authorisation from an independent

¹⁰⁰ Lassalle, (n. 2), p. 176.

¹⁰¹ *Ibid.* p. 177.

¹⁰² *Ibid.* pp. 180-181.

¹⁰³ Lasagni, (n. 17), p. 272.

¹⁰⁴ Lassalle, (n. 2), p. 182.

¹⁰⁵ Lasagni, (n. 17), p. 280.

¹⁰⁶ Blume et al., (n. 18), pp. 218, 227, 229, 236.

¹⁰⁷ *Ibid.*

¹⁰⁸ *Ibid.* p. 228.

¹⁰⁹ Lasagni, (n. 17), p. 273.

¹¹⁰ Lannier, Tosza, (n. 5), p. 307.

¹¹¹ Ni Loideain, (n. 12), p. 263.

¹¹² Kaszubowski, Steinborn, (n. 26), p. 381.

¹¹³ *Ibid.* p. 384.

body to request identification data could be compliant with the case law of the European Court of Justice (ECJ),¹¹⁴ such situation is nevertheless questionable given the lack of clear delimitation of data categories (see *supra*, Section 3.1.1)

In France, customs authorities must obtain authorisation from the public prosecutor to access data from OSPs.¹¹⁵ The authorisation of a public prosecutor is similarly required for requests to traffic data providers, telecommunication operators or other non-supervised entities by the Italian financial market supervisory authority – although a similar request under the criminal framework requires a judge authorisation.¹¹⁶ Differently, in France in the context of VAT-related investigations, financial market supervision, as well as competition enforcement, requests for data must be approved by a specialised independent body: the controller of requests for telecommunication metadata.¹¹⁷

In Germany, the access to traffic data by the financial institutions supervisors requires a court order.¹¹⁸ Specific requests for login data from telecommunications services also necessitate judicial authorisation.¹¹⁹ In Belgium, the competition and the financial markets authorities must obtain prior authorisation from an investigating judge for data access.¹²⁰ However, the access to identification data by the financial markets and data protection authorities does not require any authorisation.¹²¹ In Luxembourg, authorities in the financial institutions sectors must submit a reasoned request to an investigating judge.¹²²

3.2. General administrative powers to gather information

Aside specific powers to request data specifically from OSPs, administrative authorities are also granted general administrative powers to gather information from third parties, namely, any persons, legal or natural, not involved in the proceedings. These general powers are typically framed in technologically neutral terms, allowing authorities to request or inspect a broad range of materials, including digital data, without necessarily invoking specialised legal regimes. However, the breadth of these powers varies

¹¹⁴ ECJ, *La Quadrature du Net and Others v. Premier ministre and Ministère de la Culture*, 30.04.2024, C-470/21.

¹¹⁵ Lassalle, (n. 2), p. 176.

¹¹⁶ Lasagni, (n. 17), pp. 273.

¹¹⁷ Lassalle, (n. 2), pp. 178, 180-181, 183.

¹¹⁸ Blume et al., (n. 18), p. 228.

¹¹⁹ *Ibid.* p. 220.

¹²⁰ Franssen, Vandormael, (n. 6), p. 91.

¹²¹ *Ibid.* pp. 91, 96, 102.

¹²² Lannier, Tosza, (n. 5), p. 307.

significantly across jurisdictions. Some countries provide overarching frameworks applicable across sectors, while others rely exclusively on sector-specific provisions. Moreover, the scope of entities subject to such requests, the types of data accessible, and the procedural safeguards in place differ widely. This section offers a comparative reflection on how these general powers are structured, highlighting the tension between administrative flexibility and the need for legal certainty, especially when such powers are used to obtain electronic evidence from actors not directly subject to supervision, such as OSPs.

3.2.1. Categories of third parties as addressees to general powers to request information

Administrative authorities across various jurisdictions generally possess broad and technologically neutral powers to request and copy information or documents,¹²³ either available across various sectors or sectorial, extending their scope beyond traditional paper records to include digital data. These powers typically apply to a wide range of entities, including businesses, individuals, and third parties who may hold relevant information. Additionally, search and seizure powers, traditionally used for physical records, are increasingly being leveraged to access digital data, though they often come with stricter procedural safeguards.

Only two countries rely on powers available across various sectors. In the Netherlands, the General Administrative Law Act grants all administrative authorities the right to require ‘anyone’ to provide information and to inspect business documents and records, which in practice has been interpreted to include data.¹²⁴ In addition to these powers available across sectors, the Netherlands provides financial market authorities with the ability to request information and to obtain business documents and records from ‘anyone’ when performing statutory market surveillance duties.¹²⁵ Germany also provides for investigative powers available across sectors, namely a general investigative clause provides a broad right to request any kind of information relevant to an investigation. However, compliance is not mandatory for OSPs, reflecting a potential limitation in enforcement.¹²⁶ German law also includes a general obligation for individuals to surrender objects relevant to an investigation.¹²⁷ The German Federal Constitutional Court has interpreted that the concept of “objects” in that context includes non-tangible objects, i.e.

¹²³ The power to copy information is notably absent from the general power of the Dutch financial market authority, De Vries et al., (n. 1), p. 355.

¹²⁴ *Ibid.* p. 339.

¹²⁵ *Ibid.* p. 355.

¹²⁶ Blume et al., (n. 18), pp. 225-226.

¹²⁷ *Ibid.* p. 223.

data.¹²⁸ In addition to these powers available across sectors, Germany also regulates sector-specific powers, such as in VAT enforcement, where authorities may request information from ‘any person’,¹²⁹ and German competition authorities have the power to request information from companies, associations of companies, legal entities, and associations of persons.¹³⁰

Remaining countries rely exclusively on sectorial powers granted to administrative authorities and do not benefit from a general administrative proceedings’ framework. In France, authorities in the area of banking law and financial markets as well as the data protection authority are empowered to collect information from “any person”.¹³¹ Likewise, in Belgium, competition and financial market authorities, as well as the VAT administration,¹³² may request information from any natural or legal person;¹³³ in Luxembourg, competition, VAT and (most) financial market laws apply broadly to any person, including those holding information indirectly related to the investigated matter.¹³⁴ In Finland,¹³⁵ as well as in Italy,¹³⁶ VAT,¹³⁷ competition¹³⁸ and financial institutions authorities also have a general power to request information from third parties.¹³⁹ In Italy, the definition of customs economic operators is notably broad, extending the authorities’ powers even to third parties to the investigation, which might thus encompass OSPs.¹⁴⁰ In Poland, the competition authority may request information from any corporation, any other natural or legal person as well as organisational units.¹⁴¹

Despite these broad general powers, different restrictions on the scope of entities subject to information requests may limit the effective use of such powers to OSPs being third parties to the investigations. For example, in France, customs authorities may only request data from individuals or entities

¹²⁸ *Ibid.* p. 224.

¹²⁹ *Ibid.* pp. 226-227.

¹³⁰ *Ibid.* p. 230.

¹³¹ Lassalle, (n. 2), pp. 187, 190.

¹³² Franssen, Vandormael, (n. 6), p. 89.

¹³³ *Ibid.* p. 90.

¹³⁴ Lannier, Tosza, (n. 5), pp. 304, 309, 317.

¹³⁵ Aside administrative authorities, under the Administrative Judicial Procedure Act, the Market Court has the authority to compel the production of documents and objects as evidence in competition cases, extending this obligation to a wide range of third parties, Riekkinen, (n. 3), p. 135.

¹³⁶ Lasagni, (n. 17), pp. 275, 280.

¹³⁷ Riekkinen, (n. 3), p. 140.

¹³⁸ *Ibid.* p. 148.

¹³⁹ *Ibid.* p. 145.

¹⁴⁰ Lasagni, (n. 17), p. 278.

¹⁴¹ Kaszubowski, Steinborn, (n. 26), p. 382.

‘directly or indirectly involved’ in customs-related operations.¹⁴² Similarly, in the Netherlands, tax authorities may request information only from third parties legally required to maintain tax records, while customs authorities limit their requests to those involved in customs formalities or controls.¹⁴³ Finland¹⁴⁴ and Luxembourg¹⁴⁵ follow similar approaches, limiting customs-related requests to entities holding information necessary for customs taxation or operations. Other powers are restricted to supervised entities or related ones, which might thus exclude OSPs. In Finland, certain powers of the financial institutions supervisors are specifically designed to target supervised entities and other financial market participants, limiting the scope of information requests to those directly involved in regulated activities.¹⁴⁶ Similarly, in Luxembourg, some financial markets and banking laws restrict information requests to supervised entities, but they may also extend to persons with a direct link to supervised activities, such as auditors or other professionals involved in financial operations.¹⁴⁷

In the context of data protection enforcement, the scope of investigative powers granted under the GDPR has been extended at the national level to varying degrees across jurisdictions. While the GDPR primarily empowers authorities to request information from controllers or processors—usually understood as the investigated entity—some countries have broadened these powers to include third parties. In the Netherlands, the data protection authority may request information from ‘anyone’, extending their reach beyond the direct subjects of investigation.¹⁴⁸ Similarly, in Finland, the data protection authority may also obtain information from any third parties.¹⁴⁹ Such an extension is also contemplated in the investigation of internal rules of the Luxembourg data protection authority, although not provided for by law, raising a legality issue.¹⁵⁰ In Belgium, the data protection authority extends its reach to require the identification of the subscribers or habitual users of an electronic communication service.¹⁵¹ In contrast, Germany takes a more restrictive approach, interpreting the GDPR as conferring only general supervisory and inspection powers, without extending to administrative

¹⁴² Lassalle, (n. 2), p. 185.

¹⁴³ De Vries et al., (n. 1), p. 353.

¹⁴⁴ Riekkinen, (n. 3), p. 138.

¹⁴⁵ Lannier, Tosza, (n. 5), p. 302.

¹⁴⁶ Riekkinen, (n. 3), p. 145.

¹⁴⁷ Lannier, Tosza, (n. 5), pp. 309-310.

¹⁴⁸ De Vries et al., (n. 1), p. 362.

¹⁴⁹ Riekkinen, (n. 3), p. 154.

¹⁵⁰ Lannier, Tosza, (n. 5), p. 321.

¹⁵¹ Franssen, Vandormael, (n. 6), pp. 101-102.

punitive proceedings that could compel third parties to provide information.¹⁵²

Powers for search and seizure, traditionally used to physically obtain documents and records, can also be leveraged to request information from third parties in certain jurisdictions. For instance, in France, VAT authorities may seize ‘documents and records’ including in the form of data, under the condition of judicial authorisation. However, such powers can only be exercised if there are indications of fraud, such as issuing fictitious invoices.¹⁵³ Similarly, competition authorities may seize business records stored on any medium within business premises.¹⁵⁴ The French data protection authority may also access any location where personal data is processed, contingent on judicial approval.¹⁵⁵ Similarly, the Belgian data protection authority may perform on-site examination and consult, copy or seize computer systems containing personal data.¹⁵⁶ In Finland, competition authorities conducting on-site inspections have the right to obtain all necessary information, including from service providers managing communications or data on behalf of the investigated entity.¹⁵⁷ Belgium takes a more detailed approach, particularly regarding IT seizures during competition inspections, requiring judicial authorisation and legal representation among other requirements.¹⁵⁸ These physical document requests, which have not fully adapted to the digital nature of modern investigations, provide stronger procedural safeguards akin to those in criminal investigations, compared to general powers to request information.

As a general rule, administrative authorities across all examined jurisdictions must adhere to the principle of territoriality when exercising their investigative powers, meaning they may only request data from entities operating within their national borders. However, under German law, authorities may request data not only from entities physically established in Germany but also from any private actor providing services within the country, regardless of their physical presence. This criterion extends investigative powers beyond territorial boundaries by targeting service providers that offer services to users in Germany or merely maintain a branch in the country. Such an approach effectively broadens the scope of German authorities’ data access capabilities, allowing them to reach foreign-based companies with operations or commercial interests in Germany, thereby

¹⁵² Blume et al., (n. 18), p. 234.

¹⁵³ Lassalle, (n. 2), pp. 186-187.

¹⁵⁴ *Ibid.* pp. 187-190.

¹⁵⁵ *Ibid.* p. 190.

¹⁵⁶ Franssen, Vandormael, (n. 6), pp. 101-102.

¹⁵⁷ Riekkinen, (n. 3), p. 150.

¹⁵⁸ Franssen, Vandormael, (n. 6), p. 101-102.

circumventing strict territorial limitations typically applied in other jurisdictions.¹⁵⁹

3.2.2. Conditions to request information to third parties

The conditions for implementing general powers to request data appear to be generally less stringent than those governing specific powers. While the principle of necessity is a common denominator, its interpretation ranges from a minimal threshold of relevance to more demanding standards requiring justifiable cause or specificity. In France, for example, customs authorities may request information deemed ‘of interest’,¹⁶⁰ while under the Monetary and Financial Code, data may be obtained ‘for the purposes of the investigation’, suggesting a relatively low threshold for data requests.¹⁶¹ Similarly, in Luxembourg, customs authorities may seek ‘any information deemed necessary’,¹⁶² whereas VAT authorities may request data whenever it is necessary to detect tax infringements and ensure proper tax collection.¹⁶³

Both the Luxembourg¹⁶⁴ and Belgian¹⁶⁵ competition authorities may gather ‘necessary’ information. Finnish financial institutions authorities may obtain data from individuals who can be ‘presumed with justifiable cause’ to hold ‘necessary’ information,¹⁶⁶ and data protection authorities may request information that is necessary for fulfilling their tasks.¹⁶⁷ Luxembourg’s financial institutions authorities operate under a broader framework, allowing them to request information that may be considered likely to be relevant for their supervisory, investigatory, or other functions,¹⁶⁸ which underlines the lack of clear separation between supervisory and investigatory competences.

Similarly, the German competition authorities may use their powers either for general supervision or targeted investigations, with the latter requiring an initial suspicion. Deadlines for compliance are usually left to the discretion of the requesting authority, though German case law has deemed periods between two to four weeks to be reasonable.¹⁶⁹ In Luxembourg, VAT compliance deadlines in practice range from one week to over a month.¹⁷⁰ Italy is an exception in that the competition authorities may request all the

¹⁵⁹ Blume et al., (n. 18), p. 224.

¹⁶⁰ Lassalle, (n. 2), p. 185.

¹⁶¹ *Ibid.* p. 187.

¹⁶² Lannier, Tosza, (n. 5), p. 302.

¹⁶³ *Ibid.* p. 303.

¹⁶⁴ *Ibid.* p. 317.

¹⁶⁵ Franssen, Vandormael, (n. 6), p. 89.

¹⁶⁶ Riekkinen, (n. 3), p. 145.

¹⁶⁷ *Ibid.* p. 154.

¹⁶⁸ Lannier, Tosza, (n. 5), p. 311.

¹⁶⁹ Blume et al., (n. 18), p. 233.

¹⁷⁰ Lannier, Tosza, (n. 5), p. 303.

information deemed necessary, however, the deadline for compliance shall not exceed sixty days. This time limit may be extended upon a reasoned request.¹⁷¹ Furthermore, Italian customs authorities have the power to request information, to be provided within at least fifteen days.¹⁷²

In Poland, competition authority mostly relies on search and seizures to obtain data and enter IT systems. However, because of the principle of proportionality the exercise of this power against third party is merely subsidiary: it may only be conducted against them if the same action is not possible against the investigated person.¹⁷³

Some jurisdictions impose stricter procedural requirements in some areas of enforcement, particularly formalities related to the content of requests can also vary. In Luxembourg, competition authorities must first open a formal procedure before issuing an information request, and the request must explicitly state the object and purpose, failing which it may be declared null and void.¹⁷⁴ Requests by the German competition authorities must specify the legal basis, the object and purpose of the request, and a reasonable deadline.¹⁷⁵ Similarly, Italian competition authorities, must specify the legal grounds for the request.¹⁷⁶ In Finland, VAT-related data requests must identify the taxpayer by name, bank account number, or another specific identifier, preventing fishing expeditions but allowing for requests without personal identification if other specific details are provided;¹⁷⁷ and in Finland's financial institutions sector, data requests are usually issued in writing, specifying the information sought and the legal basis for the request.¹⁷⁸ In Germany, VAT data requests follow a layered approach, targeting any person and subsidiarily the taxpayer for taxation purposes.¹⁷⁹

3.2.3. Categories of data under general powers

The general powers, as previously defined, are not confined to specific sectors or to specific categories of actors, and are typically framed in broad, technologically neutral terms. As a result, they often allow authorities to request a wide range of data, from traditional business records to digital content such as emails, metadata, or system logs. However, the breadth and precision of these powers vary significantly across jurisdictions. Some legal

¹⁷¹ Lasagni, (n. 17), p. 276.

¹⁷² *Ibid.* p. 279.

¹⁷³ Kaszubowski, Steinborn, (n. 26), p. 384.

¹⁷⁴ Lannier, Tosza, (n. 5), p. 318.

¹⁷⁵ Blume et al., (n. 18), p. 232.

¹⁷⁶ Lasagni, (n. 17), p. 276.

¹⁷⁷ Riekkinen, (n. 3), p. 141.

¹⁷⁸ *Ibid.* p. 146.

¹⁷⁹ Blume et al., (n. 18), pp. 226-227.

systems explicitly include digital formats and define the scope of accessible data in detail, while others rely on vague or outdated terminology, leaving room for interpretation. Moreover, the extent to which sensitive or privileged data can be accessed under general powers is unevenly regulated.

The breadth of categories of data that can be requested under general powers is extensive across various jurisdictions, encompassing both paper and digital formats. In the Netherlands, authorities may request a wide array of ‘records’, which includes data such as GPS registrations, email data, mailboxes, USBs, and even more specific items such as draft accounts, till rolls, microfilms, and order confirmations.¹⁸⁰ The Dutch data protection authority may explicitly request telemetry data, which covers information about the transmission of personal data to other devices.¹⁸¹ In Luxembourg, customs authorities may obtain documents and correspondence,¹⁸² while the VAT authority, like in Ireland,¹⁸³ may demand all information related to taxable operations.¹⁸⁴ The French data protection authority may request all types of documents and even computer programs.¹⁸⁵ Finnish competition and data protection authorities are likewise empowered to request all types of data.¹⁸⁶ Also Italian authorities may obtain copies of all types of documents, including access to databases.¹⁸⁷

The breadth of the scope is particularly extensive for competition and financial institutions authorities. In Germany, competition authorities may demand all original documents in any form, including data storage locations and passwords,¹⁸⁸ as long as the data is accessible within the economic unit.¹⁸⁹ Belgium grants competition authorities the power to access digital evidence, such as electronic and instant messages, irrespective of their storage location, whether on local servers or in the cloud.¹⁹⁰ The Dutch competition authority further clarifies that its data requests may include content and metadata as long as related to business information, such as emails, chat applications, and document edits.¹⁹¹ In Luxembourg, the financial institutions authorities,¹⁹² as well as the competition authority, may access any document, information, or

¹⁸⁰ De Vries et al., (n. 1), pp. 340, 353.

¹⁸¹ *Ibid.* p. 363.

¹⁸² Lannier, Tosza, (n. 5), p. 302.

¹⁸³ Ni Loideain, (n. 12), p. 262.

¹⁸⁴ Lannier, Tosza, (n. 5), p. 303.

¹⁸⁵ Lassalle, (n. 2), p. 190.

¹⁸⁶ Riekkinen, (n. 3), pp. 148, 154.

¹⁸⁷ Lasagni, (n. 17), p. 284.

¹⁸⁸ Blume et al., (n. 18), p. 230.

¹⁸⁹ *Ibid.* p. 232.

¹⁹⁰ Franssen, Vandormael, (n. 6), p. 99.

¹⁹¹ De Vries et al., (n. 1), pp. 357-358.

¹⁹² Lannier, Tosza, (n. 5), p. 310.

data available to the addressee, including software data for the latter.¹⁹³ Finland explicitly includes recordings of telephone conversations, electronic communications, telecommunications data, and information systems within the scope of data requests by the financial institutions authorities.¹⁹⁴ The Italian competition authority may access all electronic communications, including recordings,¹⁹⁵ the customs authority may access all data and documents related to taxes in the broad sense,¹⁹⁶ while the VAT authority may demand documents and invoices relating to transactions.¹⁹⁷

However, such broad scopes are restricted in some jurisdictions based on a balancing exercise with the protection of fundamental rights. Some of these restrictions derive from the same legislations on administrative proceedings. In France, customs and financial market authorities have broad powers to access ‘papers and documents, whatever the medium’, implying an all-encompassing scope that includes data.¹⁹⁸ However, the scope must exclude telecommunication metadata, which request is specifically regulated under a different power (see Section 2.1). In Finland, traffic and content data related to electronic communications may only be acquired from supervised entities, limiting the scope of data requests in the financial institutions sector.¹⁹⁹

Furthermore, all jurisdictions restrict the scope of the gathering of information through the protection of different professional secrecy. In the Netherlands, authorities cannot request personal or non-business documents, and business documents covered by legal professional privilege are also protected. Dutch law recognises the secrecy of information received by lawyers,²⁰⁰ as well as similar protections for clergymen, notaries, doctors, and pharmacists in tax matters.²⁰¹ Similarly, Germany imposes stricter frameworks and guarantees for data that require heightened protection, such as due to the legal professional privilege.²⁰² Conversely, Luxembourg’s financial institutions laws prevent the use of professional secrecy to refuse cooperation, except in market abuse cases.²⁰³ In Finland, certain individuals have a general right not to testify, such as due to a professional secrecy;

¹⁹³ *Ibid.* p. 317.

¹⁹⁴ Riekkinen, (n. 3), p. 145.

¹⁹⁵ Lasagni, (n. 17), p. 275.

¹⁹⁶ *Ibid.* pp. 278-279.

¹⁹⁷ *Ibid.* p. 280.

¹⁹⁸ Lassalle, (n. 2), pp. 185-187.

¹⁹⁹ Riekkinen, (n. 3), p. 146.

²⁰⁰ De Vries et al., (n. 1), p. 341.

²⁰¹ *Ibid.* pp. 345-346.

²⁰² Blume et al., (n. 18), p. 224.

²⁰³ Lannier, Tosza, (n. 5), p. 312.

however, this does not extend to disclosing information about their financial situation in customs and VAT matters.²⁰⁴

However, there is no standardised regulatory framework for filtering privileged data in any of the studied jurisdiction, except in the Netherlands. The Dutch financial market authorities have implemented a binding regulation detailing a multi-step process to clean data, involving IT specialists, notification to the investigated party, and possible remedies before civil courts.²⁰⁵ A different approach is followed by the Dutch competition and data protection authorities, which establish a ‘within-the-scope’ dataset before allowing an overview to the concerned person, who can then request filtering of potentially irrelevant information, subject to review by a legal professional privilege officer.²⁰⁶ In France, the data protection authority is restricted from accessing data protected by legal professional secrecy, journalistic secrecy, and medical secrecy.²⁰⁷

In addition to sector-specific and procedural restrictions, the scope of administrative authorities’ investigative powers is also limited by constitutional and European frameworks that limit data collection. In the Netherlands, the Supreme Court has ruled that intrusive investigative techniques, such as placing GPS trackers on vehicles or accessing automatic license plate recognition systems used by the police, are not permissible for administrative enforcement purposes, as they constitute a serious interference with private life under European Court of Human Rights (ECtHR) case law.²⁰⁸ Furthermore, Dutch authorities face restrictions in accessing traffic and location data, which is primarily reserved for criminal proceedings and requires prior judicial authorisation.²⁰⁹

Similarly, in Finland, the Constitution allows for limitations on the secrecy of communications for criminal investigations but does not extend the same permissions to punitive administrative proceedings. Finnish constitutional doctrine establishes that administrative investigations cannot, in practice, employ covert measures equivalent to telecommunications interception or traffic data monitoring.²¹⁰ Luxembourg and Germany impose notable constitutional and statutory limits on administrative access to electronic communication data, reserving it for criminal proceedings and excluding professional data from constitutional coverage.²¹¹ Germany applies

²⁰⁴ Riekkinen, (n. 3), pp. 138, 140.

²⁰⁵ De Vries et al., (n. 1), pp. 355-357.

²⁰⁶ *Ibid.* pp. 360-362.

²⁰⁷ Lassalle, (n. 2), p. 191.

²⁰⁸ De Vries et al., (n. 1), p. 343.

²⁰⁹ *Ibid.* p. 344.

²¹⁰ Riekkinen, (n. 3), p. 146.

²¹¹ Lannier, Tosza, (n. 5), pp. 324-325.

a ‘double-door model’, requiring both a legal basis for the authority’s request and a separate one for the OSP’s disclosure.²¹²

3.3. Transfer of data and enforcement of orders

This section explores how administrative authorities across jurisdictions operationalise their powers to gather electronic evidence, focusing on two key dimensions: the transfer of data and the enforcement of requests when OSPs do not conform to these. The comparative analysis reveals that while some jurisdictions have developed secure and formalised systems for data transmission, others rely on informal or inconsistent practices. Similarly, enforcement mechanisms vary widely: some legal systems provide strong coercive tools such as fines, administrative penalties, or even criminal sanctions, while others offer limited or no means to compel third-party cooperation, which is similar to criminal law.²¹³ These disparities affect not only the efficiency of administrative investigations but also the legal certainty and accountability of data collection practices.

3.3.1. Data transfer

The transfer of data requested by administrative authorities under both general and specific powers is subject to relatively few formal conditions and rules across jurisdictions. the transfer of data, once requested by administrative authorities, is diversely regulated and implemented in practice across jurisdictions. Indeed, the analysis reveals a fragmented landscape: while some countries have implemented secure and formalised channels, such as encrypted platforms or structured formats, others rely on *ad hoc* methods like email or postal delivery, often lacking consistency and reliability. Requirements concerning the readability, confidentiality, and integrity of transferred data also vary, with only a few jurisdictions imposing clear obligations on format or ensuring that sensitive data is adequately protected during transmission. Moreover, rules on data retention and destruction are often sector-specific and inconsistently applied, raising concerns about proportionality and long-term data protection. These divergences highlight the operational challenges of digital evidence gathering and underscore the need for clearer, harmonised standards to ensure both the effectiveness and the accountability of administrative data transfers.

In Germany, subscriber data must be transferred ‘without delay and at the requesting party’s expense’, with a requirement to maintain confidentiality regarding the request. Additionally, telecommunications

²¹² Blume et al., (n. 18), pp. 212-213.

²¹³ Franssen, Tosza, (n. 76).

service providers with more than 100,000 customers must ensure a secure electronic interface for data transfer, which can take the form of an email-based procedure or a dedicated electronic platform.²¹⁴ For competition matters, data must be provided electronically via an online platform.²¹⁵ In Finland, customs, data protection and VAT-related data requests must also be transferred at the entity's expense.²¹⁶ In France, the VAT authority mandates data transmission through a secure system.²¹⁷ In Luxembourg, VAT-related data may be exchanged through a dedicated platform provided by the administrative authority when large data volumes are involved. However, in practice, the platform seems to be oftentimes unreliable, resulting in data being transferred via email, post, or a combination of both.²¹⁸

Regarding the format of transferred data, several jurisdictions impose requirements to ensure accessibility of computer programs and data. In France, the data protection authority mandates that such information should be transcribed into a format that is intelligible.²¹⁹ Similarly, Luxembourg's customs and VAT laws require data to be provided in a readable and comprehensible form.²²⁰ Luxembourg competition authority may request that data be transcribed into documents.²²¹ The Luxembourg competition authority further specifies that data must be provided in a clear way, meaning it should not be encrypted.²²² The Netherlands also incorporates encryption measures in competition investigations, by applying a hash to ensure the integrity and security of the dataset throughout the process.²²³

Examined legal orders provide also rules as regards protection of data collected by administrative authorities as well its mandatory destruction. In France, the VAT law requires storage measures that guarantee confidentiality.²²⁴ Similarly, the financial markets authority imposes strict storage protocols to preserve confidentiality,²²⁵ while the competition authority ensures that data is both transmitted and stored securely.²²⁶ In Germany, telecommunications service providers must provide a secure electronic interface that safeguards data integrity and maintains logs to track

²¹⁴ Blume et al., (n. 18), pp. 220-221.

²¹⁵ *Ibid.* p. 230.

²¹⁶ Riekkinen, (n. 3), pp. 139, 141, 154.

²¹⁷ Lassalle, (n. 2), p. 178.

²¹⁸ Lannier, Tosza, (n. 5), p. 303.

²¹⁹ Lassalle, (n. 2), p. 190.

²²⁰ Lannier, Tosza, (n. 5), pp. 302, 303.

²²¹ *Ibid.* p. 317.

²²² *Ibid.*

²²³ De Vries et al., (n. 1), p. 360.

²²⁴ Lassalle, (n. 2), p. 178.

²²⁵ *Ibid.* p. 182.

²²⁶ *Ibid.* p. 184.

access.²²⁷ In Finland, in cases involving large datasets, practical aspects such as data security and pseudonymisation are typically discussed in advance between the competition authority and the responding party to address potential challenges before an official request is made.²²⁸

With regard to data destruction, few jurisdictions have set time limits for how long data can be stored, and those rules are usually provided on sectoral level. In France, customs data must be deleted once tax penalties are enforced,²²⁹ while VAT-related data must be retained for one year or until the conclusion of all appeal procedures.²³⁰ The financial markets authority requires data to be destroyed one month after the Board's decision or six months after the final ruling of the Enforcement Committee or appeal courts if a notification of grievance has been issued; however, data transferred to criminal proceedings may be retained for longer.²³¹ The competition authority follows a similar approach, with data deleted six months after a final decision or within one month if the information pertains to facts that are not prosecuted.²³² In the Netherlands, the financial markets authority's working methods specify that raw data should be deleted once a clean dataset has been produced, or if it is determined that certain data should have been excluded from the investigation.²³³

3.3.2. Enforcement of requests

While administrative authorities across jurisdictions are increasingly empowered to request data from third parties, the effectiveness of these powers ultimately depends on the availability and strength of enforcement mechanisms to ensure compliance: mechanisms that vary widely in scope, intensity, and applicability. The enforcement of administrative authorities' data requests is typically executed by means of general statutory obligations to cooperate, applying both to specific and general powers. Coercive fines or penalty payments are used to ensure compliance under some legal frameworks.

The enforcement of data requests through coercive fines varies widely across jurisdictions in both scope and severity. Some countries, such as Germany²³⁴ and Luxembourg,²³⁵ impose substantial financial penalties—

²²⁷ Blume et al., (n. 18), p. 221.

²²⁸ Riekkinen, (n. 3), p. 150.

²²⁹ Lassalle, (n. 2), p. 176.

²³⁰ *Ibid.* p. 178.

²³¹ *Ibid.* p. 181.

²³² *Ibid.* p. 184.

²³³ De Vries et al., (n. 1), pp. 356-357.

²³⁴ Blume et al., (n. 18), p. 234.

²³⁵ Lannier, Tosza, (n. 5), p. 318.

often calculated as a percentage of a company's global turnover—for non-compliance, particularly in competition law. Ireland²³⁶ and Italy²³⁷ provide for high maximum coercive fines in the financial and competition sectors. France²³⁸ and Luxembourg²³⁹ also apply daily fines, though in Luxembourg these are often limited to supervised entities, excluding third parties like OSPs.²⁴⁰ In contrast, Finland adopts a more cautious model: fines require judicial approval or are only imposed in cases of non-negligent non-compliance.²⁴¹ Meanwhile, the Netherlands stands out for lacking coercive fines altogether in this context.²⁴²

In some jurisdictions, failure to comply with data requests does not result in any sanctions, particularly for third parties, effectively relying on voluntary cooperation. For instance, in Poland, no specific enforcement measure exists.²⁴³ In Italy, no enforcement mechanisms is provided for specific request of data by the financial supervisor.²⁴⁴ In the Netherlands, under competition and data protection laws, only the investigated party may be sanctioned, not third parties.²⁴⁵ Similarly, Finnish competition authority may impose fines for providing false, insufficient, or misleading information, but these are typically limited to undertakings under investigation, making their applicability to third parties unlikely according to the literature.²⁴⁶ Raising the same question, the Luxembourg competition authority, as well as the Italian competition authority,²⁴⁷ may impose fines to undertakings, understood as those under investigation and not third parties, if failing to comply with a request for information.²⁴⁸

Administrative fines for non-compliance with data requests vary widely in amount, scope, and legal basis across jurisdictions. The general tendency shows low fines under customs frameworks, compared to highest ones available to competition and financial regulators. France and Luxembourg impose sector-specific fines ranging from modest daily penalties (e.g., €150 in French customs or €250–10,000 in Luxembourg VAT)²⁴⁹ to substantial

²³⁶ Ni Loideain, (n. 12), p. 255.

²³⁷ Lasagni, (n. 17), p. 276.

²³⁸ Lassalle, (n. 2), p. 176.

²³⁹ Lannier, Tosza, (n. 5), p. 304.

²⁴⁰ *Ibid.* p. 312.

²⁴¹ Riekkinen, (n. 3), p. 146, 151.

²⁴² De Vries et al., (n. 1), p. 342.

²⁴³ Kaszubowski, Steinborn, (n. 26), pp. 384–385.

²⁴⁴ Lasagni, (n. 17), p. 274.

²⁴⁵ De Vries et al., (n. 1), pp. 359, 364.

²⁴⁶ Riekkinen, (n. 3), p. 152.

²⁴⁷ Lasagni, (n. 17), p. 274.

²⁴⁸ Lannier, Tosza, (n. 5), p. 318.

²⁴⁹ *Ibid.* p. 304.

amounts in financial sectors—up to €5 million or 10% of annual turnover.²⁵⁰ Germany combines low general fines with higher competition-related penalties,²⁵¹ while Italy's VAT and financial regulators may impose fines up to €8,000 and €5 million respectively.²⁵² In Finland, fines are more moderate and often tied to negligence, with a €15,000 cap in VAT enforcement.²⁵³

In some jurisdictions, failure to comply with administrative data requests may trigger criminal liability, though the scope and severity of sanctions vary considerably. The Netherlands criminalises general non-cooperation, including by third parties and OSPs, with penalties up to three months' imprisonment.²⁵⁴ France²⁵⁵ and Luxembourg impose criminal penalties across multiple sectors, with fines reaching up to €125,000 and prison sentences of up to five years, particularly in financial and securities regulation.²⁵⁶ Italy applies criminal sanctions more selectively—typically for providing false information or obstructing investigations—with VAT-related violations carrying prison terms of up to seven years.²⁵⁷

4. LEGAL SAFEGUARDS IN ADMINISTRATIVE INVESTIGATION PROCEEDINGS

Legal safeguards in administrative investigation proceedings are unevenly developed across jurisdictions, particularly when it comes to protecting third parties such as OSPs. While most legal systems formally recognise core principles, like the right to be heard, protection against self-incrimination, and access to remedies, their practical application is often limited or unclear. Safeguards tend to focus on the investigated person, leaving third parties with limited procedural rights and unclear guidance on how to challenge data requests. Judicial oversight is rarely available at the request stage, and remedies typically become accessible only once enforcement measures are imposed. Moreover, the legal status of data requests, whether they constitute appealable acts or mere preparatory steps, varies significantly, affecting the availability of procedural protections. Overall, the analysis reveals a structural gap between the expanding powers of administrative authorities to gather electronic evidence and the underdeveloped framework of safeguards designed to ensure fairness, transparency, and accountability in such proceedings.

²⁵⁰ *Ibid.* pp. 313-314.

²⁵¹ Blume et al., (n. 18), pp. 221-222, 234.

²⁵² Lasagni, (n. 17), pp. 281-283.

²⁵³ Riekkinen, (n. 3), p. 143.

²⁵⁴ De Vries et al., (n. 1), p. 342.

²⁵⁵ Lassalle, (n. 2), p. 184.

²⁵⁶ Lannier, Tosza, (n. 5), p. 314.

²⁵⁷ Lasagni, (n. 17), pp. 279, 281.

4.1. Safeguards available to third parties

Safeguards available to third parties against data requests by administrative authorities are quite limited under all studied jurisdictions and remain diverse among areas of enforcement and between specific and general powers. Some safeguards indirectly extend to third parties, including OSPs, even though they are not the primary focus of the legal frameworks. For instance, certain provisions aim to uphold the principle of non-self-incrimination when data requests risk revealing unrelated violations, while others require notification, often through record-keeping, and offer a limited right to be heard. Remedies are generally designed for the investigated person, but in some jurisdictions, they are formulated broadly enough to be invoked by third parties, including OSPs, when they are asked to produce data. However, the applicability of these safeguards to third parties remains legally ambiguous and inconsistently recognised, reflecting a broader structural gap in procedural protections for actors who are not the direct subject of investigation but are nonetheless instrumental in the evidence-gathering process.

4.1.1. Protection against self-incrimination

Examined legal orders included protection against self-incrimination of the requested third parties into proceedings in which administrative authorities gather data from third parties. This safeguard derives from the ECtHR *Saunders* case law, incorporated into national administrative punitive proceedings.²⁵⁸

For instance, in the Netherlands, if an investigation into a particular entity reveals potential violations by third parties, the authority refrains from expanding the ongoing investigation to include them. Instead, it initiates a separate enforcement procedure to ensure that third parties do not inadvertently become subjects of investigation without proper procedural safeguards.²⁵⁹ Yet, third parties in the Netherlands are not protected by the privilege against self-incrimination unless the requested information directly implicates them in wrongful conduct.²⁶⁰ This privilege is mostly recognised in favour of the investigated person, but it is limited to will-dependent acts. However, the privilege does not extend to documentary evidence, such as passwords or biometric data, which are considered will-independent and can be requested without violating the privilege. For instance, in competition

²⁵⁸ ECtHR, *Saunders v. the United Kingdom*, 17.12.1996, no. 19187/91; S. Lamberigts, *Corporations and the privilege against self-incrimination*, Hart Publishing, Hart Studies in European Criminal Law, 2022.

²⁵⁹ De Vries et al., (n. 1), p. 364.

²⁶⁰ *Ibid.* pp. 346-347.

investigations, authorities are required to inform employees of the natural person under investigation of their rights, ensuring they have an opportunity to invoke the privilege.²⁶¹ Conversely, in Poland, the law explicitly allows to use data disclosed against the person at the origin of the disclosure, although the provision only refers to natural persons.²⁶²

Similarly, in France, the financial markets authority is explicitly authorised to implement its specific power to request data solely for the purposes of the investigation for which it has received prior authorisation, preventing any unauthorised expansion of the inquiry's scope.²⁶³ In Finland, coercive fines are excluded in customs matters when their imposition could jeopardise the privilege against self-incrimination, while in sectors such as banking, financial markets, competition, and data protection, this safeguard applies only to natural persons.²⁶⁴ In Luxembourg, the sanctioning of supervised entities in the financial institutions sector for failing to provide potentially self-incriminating information has faced criticism from legal scholars and the State Council, reflecting concerns over the balance between regulatory compliance and fundamental rights.²⁶⁵ Additionally, in Luxembourg²⁶⁶ and Italy's²⁶⁷ competition law frameworks, requests for data must not compel undertakings to admit the existence of an infringement.

4.1.2. Notification and right to be heard

The right to be notified and to be heard are foundational principles of fair administrative proceedings, yet their application in the context of data requests to OSPs remain inconsistent and often underdeveloped. While some jurisdictions formally recognise these rights and provide mechanisms for their implementation, such as prior communication of the grounds for a decision or the opportunity to submit observations, others treat data requests as mere investigatory acts, not triggering procedural safeguards. Even where safeguards exist, they are often designed with the investigated person in mind, leaving third parties with limited or unclear entitlements.

Other safeguards relate to the recording and notification of data requests when administrative authorities obtain data from third parties. For example, in France, customs authorities are required to maintain records when exercising their specific power to obtain data from OSPs.²⁶⁸ Similarly, in

²⁶¹ *Ibid.* p. 359.

²⁶² Kaszubowski, Steinborn, (n. 26), p. 388.

²⁶³ Lassalle, (n. 2), p. 181.

²⁶⁴ Riekkinen, (n. 3), pp. 139, 146, 151, 156.

²⁶⁵ Lannier, Tosza, (n. 5), p. 313.

²⁶⁶ *Ibid.* p. 318.

²⁶⁷ Lasagni, (n. 17), p. 276.

²⁶⁸ Lassalle, (n. 2), p. 176.

Luxembourg, customs authorities operating under their general powers must provide the owner of the record with a detailed list of the materials collected.²⁶⁹

Similarly, the right to be heard, while being an essential procedural safeguard in administrative sanctioning proceedings is often recognised as a general principle of administrative procedure especially when the sanction is qualified as criminal,²⁷⁰ for instance in Poland.²⁷¹ In Finland²⁷² and in Belgium,²⁷³ the Market Court, which is a judicial and not an administrative authority, ensures this right by allowing parties to present their views before issuing a production order. In Luxembourg, the framework for non-contentious administrative procedures mandates authorities to communicate the factual and legal grounds of their decisions, granting individuals eight days to submit their observations. Luxembourgish case law further emphasises that the right must be specifically detailed, rather than merely mentioned, particularly in financial sector investigations. However, failure to comply with this requirement only results in the annulment of a decision if it can be demonstrated that proper consideration would have led to a different outcome.²⁷⁴ In the context of customs enforcement, Luxembourg authorities must provide prior communication of the grounds for unfavourable decisions, such as imposing an administrative fine for failure to comply with an information request, and allow a 30-day period for observations.²⁷⁵ In competition law, Luxembourg authorities ensure that undertakings are notified of the objections raised against them and are given at least one month to submit their observations before the imposition of coercive or administrative fines.²⁷⁶

4.1.3. Remedies

The availability of remedies for third parties subject to data requests by administrative authorities presents significant challenges, primarily due to the uncertain legal status of such requests. In contrast, in certain jurisdictions and areas of enforcement, there are no specific remedies available to third parties. For instance, in France, the law does not provide for any remedies for third

²⁶⁹ Lannier, Tosza, (n. 5), p. 302.

²⁷⁰ European Court of Human Rights, *Guide on Article 6 of the European Convention on Human Rights Right to a fair trial (criminal limb)*, Council of Europe, 31.08.2022; Committee of Ministers, *Resolution (77) 31 on protection of the individual in relation to the acts of administrative authorities*, Council of Europe, 28.09.1977.

²⁷¹ Kaszubowski, Steinborn, (n. 26), p. 384.

²⁷² Riekkinen, (n. 3), p. 136.

²⁷³ Franssen, Vandormael, (n. 6), p. 100.

²⁷⁴ Lannier, Tosza, (n. 5), p. 298.

²⁷⁵ *Ibid.* p. 303.

²⁷⁶ *Ibid.* p. 319.

parties against requests for data made under both specific and general powers by authorities such as customs,²⁷⁷ VAT administration,²⁷⁸ and the financial markets authority.²⁷⁹

A key issue is whether these requests constitute administrative acts that may be challenged directly or if they are merely preparatory measures that do not provide an immediate right of appeal. In the Netherlands, the distinction is made between administrative decisions—defined as written decisions by an administrative body with legal effects—and factual acts. The latter may only be challenged if they contribute to the motivation of a final decision.²⁸⁰ As a last resort, civil courts provide a safety net through tort actions, offering stringent judicial review to scrutinise the actions of public authorities under public law principles.²⁸¹ Similarly, in Luxembourg, competition law case law treats requests for information as mere investigatory steps rather than final administrative decisions, thereby denying third parties immediate remedies,²⁸² a limitation justified by courts by the need for enforcement efficiency.²⁸³ In Finland, the situation is comparable, with requests for evidence generally not considered appealable decisions.²⁸⁴ For instance, in VAT enforcement,²⁸⁵ an initial written request does not carry the legal weight of an administrative decision, and in the financial institutions sector, ignoring such requests does not entail direct consequences.²⁸⁶ This approach extends to competition and data protection enforcement, where only enforcement actions such as coercive fines trigger appeal rights.²⁸⁷ The main advantage of this approach for authorities is that such requests are typically prepared and sent by the same investigator, often without any judicial or administrative oversight until enforcement becomes necessary.

To the contrary, remedies are available against requests if they require authorisation. Germany excludes preparatory investigative measures from appeal, but only if they lack legal significance and do not interfere with an individual's legal sphere.²⁸⁸ However, judicial orders authorising investigatory measures during administrative proceedings may be subject to judicial review. If an order is issued by an administrative authority court

²⁷⁷ Lassalle, (n. 2), pp. 176, 186.

²⁷⁸ *Ibid.* p. 180.

²⁷⁹ *Ibid.* p. 182.

²⁸⁰ De Vries et al., (n. 1), p. 349.

²⁸¹ *Ibid.* pp. 351-352.

²⁸² Lannier, Tosza, (n. 5), p. 297.

²⁸³ *Ibid.* p. 320.

²⁸⁴ Riekkinen, (n. 3), p. 137.

²⁸⁵ *Ibid.* p. 140.

²⁸⁶ *Ibid.* p. 146.

²⁸⁷ *Ibid.* pp. 149, 155.

²⁸⁸ Blume et al., (n. 18), p. 215.

review is available only if explicitly provided by law. There remains theoretical uncertainty regarding whether a third party may make use of such a remedy based on a legitimate interest, such as the disclosure of personal data.²⁸⁹ A similarly unclear situation can be found in Luxembourg as regards the third persons as the remedies seem to exclude them.²⁹⁰ In France, judicial review is available if an order is issued by a judicial authority, e.g. in customs matters.²⁹¹ Naturally, remedies remain available against administrative decisions, particularly in case of enforcement of data requests, such as through coercive fines. Remedies are available against Dutch administrative decisions through internal administrative review, followed by an indirect appeal to an administrative court.²⁹² In Belgium, decisions made by administrative authorities in competition, financial institutions, and data protection matters—such as administrative fines—can be appealed before the Market Court, which provides judicial oversight.²⁹³ Similarly, in Germany, third parties may seek judicial review against administrative fines, which are considered administrative acts.²⁹⁴ In Finland, remedies generally consist of an administrative review followed by judicial review.²⁹⁵ Some areas, such as VAT enforcement, require a mandatory administrative review by the Adjustment Board before the matter may proceed to judicial review.²⁹⁶ In Luxembourg, there are multiple layers of administrative recourse against sanctions, including requesting a reassessment by the issuing authority, escalating to a hierarchical superior (e.g., a director), or appealing to the supervising authority (e.g., a ministry). Judicial review is available against any of these administrative decisions, provided that the third party can demonstrate a ‘personal, direct, and legitimate interest’.²⁹⁷ However, in the financial institutions sector, some legal frameworks only provide for a review of the substance of the case rather than the merits, limiting the scope of challenges.²⁹⁸

4.2. Safeguards available to the investigated person

Safeguards available to the investigated person in administrative proceedings often stem from fundamental rights principles, yet they are not always explicitly enshrined in the relevant legal frameworks. This lack of

²⁸⁹ *Ibid.* pp. 214-215, 222.

²⁹⁰ Lannier, Tosza, (n. 5), p. 307.

²⁹¹ Lassalle, (n. 2), pp. 178, 180-181, 183.

²⁹² De Vries et al., (n. 1), p. 348.

²⁹³ Franssen, Vandormael, (n. 6), p. 99.

²⁹⁴ Blume et al., (n. 18), p. 208.

²⁹⁵ Riekkinen, (n. 3), p. 137.

²⁹⁶ *Ibid.* p. 144.

²⁹⁷ Lannier, Tosza, (n. 5), p. 300.

²⁹⁸ *Ibid.* p. 316.

explicit recognition and detailed regulation raises concerns regarding legal certainty and predictability for individuals facing investigation. While some safeguards overlap with those afforded to third parties (see Section 3.1), the investigated person benefits from additional protections due to their direct involvement in the proceedings. These additional safeguards, however, remain inconsistently applied across jurisdictions and enforcement areas, leading to potential disparities in protection.

The right to notification and access to records in favour of investigated persons also varies across jurisdictions. In France, under customs law, records obtained through specific investigatory powers are systematically added to the case file.²⁹⁹ In Germany, the investigated person must be notified of court decisions that affect their rights, such as requests for login data. However, there is no obligation to notify them of investigative actions taken by the public prosecution, police, or administrative authority.³⁰⁰ When subscriber data is requested, notification is only required once it no longer risks compromising the investigation's purpose.³⁰¹ In the absence of notification, the fair trial principle is ensured through access to the file.³⁰² Furthermore, in cases of voluntary surrender or seizure of data, both the data holder (e.g., OSP) and the affected individual must be notified.³⁰³ Luxembourg's framework on non-contentious administrative procedures grants individuals the right to access their administrative files, with exceptions for public or private interests.³⁰⁴ However, in practice, access to records is often denied or not provided in VAT matters.³⁰⁵ In competition law, the principle of access is upheld, but exceptions apply, such as legal privilege protecting communications between lawyers and their clients.³⁰⁶

The right to be heard is a fundamental safeguard ensuring that the investigated person may present their side before adverse decisions are made. In Germany, the accused must be heard before any evidence is used against them in court proceedings.³⁰⁷ In Finland, the right to be heard extends broadly to claims and evidence, requiring authorities to notify the investigated person before an administrative sanction is imposed or before a proposal for sanctions is submitted to the court. Finland also provides broad access rights to documents held by public authorities that may be relevant to the case.³⁰⁸

²⁹⁹ Lassalle, (n. 2), p. 176.

³⁰⁰ Blume et al., (n. 18), p. 214.

³⁰¹ *Ibid.* p. 220.

³⁰² *Ibid.* p. 222.

³⁰³ *Ibid.* p. 224.

³⁰⁴ Lannier, Tosza, (n. 5), p. 298.

³⁰⁵ *Ibid.* p. 305.

³⁰⁶ *Ibid.* p. 320.

³⁰⁷ Blume et al., (n. 18), p. 214.

³⁰⁸ Riekkinen, (n. 3), p. 137.

Luxembourg's legal framework formally upholds the right to be heard, requiring authorities to notify undertakings of the objections raised against them and allowing at least a month for their observations.³⁰⁹ However, in practice, the right is not always fully respected in areas such as VAT enforcement, where individuals might not receive adequate notice or are refused the opportunity to respond.³¹⁰ In Ireland, the right to be heard extends to all administrative bodies when they are exercising any powers related to the administration of justice.³¹¹

The availability and effectiveness of remedies for investigated persons differ significantly across jurisdictions. In the Netherlands, remedies available to third parties are also accessible to investigated persons, including interim relief proceedings to challenge the relevance or nature of data obtained by administrative authorities. Dutch case law has established that individuals may challenge the inclusion of private or privileged information in the evidence obtained during investigations.³¹² Similarly, in Germany, remedies for investigated persons align with those available to third parties. In Luxembourg, VAT-related cases allow for administrative or judicial complaints to be filed with the civil tribunal. However, issues arise regarding the lack of legal personality of the tax authority, complicating the process.³¹³ In contrast, France follows a different approach, where individuals cannot challenge the legality of investigatory measures until the information obtained is used as evidence against them. French case law permits affected persons to sue the state in cases of serious misconduct. However, the lack of immediate recourse during the investigative phase limits procedural safeguards and oversight.³¹⁴ In contrast, Irish law provides a statutory right of appeal from most administrative authorities.³¹⁵

5. TRANSFER AND ADMISSIBILITY OF DATA OBTAINED FROM ADMINISTRATIVE INVESTIGATION POWERS

This section examines the legal frameworks governing the transfer and admissibility of electronic evidence obtained by administrative authorities from OSPs across the studied jurisdictions. The comparative analysis reveals a fragmented and often underdeveloped regulatory landscape, where sector-specific rules, informal cooperation mechanisms, and general administrative principles coexist with limited harmonisation. While most jurisdictions

³⁰⁹ Lannier, Tosza, (n. 5), p. 305.

³¹⁰ *Ibid.* p. 319.

³¹¹ Ni Loideain, (n. 12), p. 249.

³¹² De Vries et al., (n. 1), p. 352.

³¹³ Lannier, Tosza, (n. 5), p. 304.

³¹⁴ Lassalle, (n. 2), p. 193.

³¹⁵ Ni Loideain, (n. 12), p. 249.

adhere to the principle of free evaluation of evidence, the admissibility of data gathered from third parties is subject to varying degrees of procedural safeguards, particularly when such data is transferred between administrative and criminal proceedings or across borders. The section highlights significant disparities in the availability of enforcement mechanisms, the protection of fundamental rights, and the legal certainty afforded to both investigated persons and third parties. These findings underscore the pressing need for clearer, more coherent standards to ensure the effective and accountable use of electronic evidence in administrative punitive enforcement.

5.1. The transfer of data obtained from third parties

In all studied countries, there are no specific rules on the transfer of data obtained from third parties, notably OSPs. The research identified diverse legal bases concerning transfer of evidence between proceedings. The rules governing the sharing of data vary widely depending on the authority involved, the sector in question, and the intended purpose of the transfer.

5.1.1. Transfer of evidence at national level

One of the key concerns regarding the transfer of evidence at the national level is the close interaction between administrative and criminal proceedings, leading to potential risks of circumventing the procedural safeguards specific to criminal investigations. In most jurisdictions, there is no general framework governing these transfers. Luxembourg has a legal framework for inter-administrative and judicial cooperation, though it primarily concerns customs and tax administrations.³¹⁶ Nevertheless, some similar rules can be found in several investigated countries among diverse sectors.

The existence and scope of official secrecy for administrative authorities vary across jurisdictions, with some countries imposing stricter confidentiality rules than others. In the Netherlands, tax secrecy is particularly stringent, restricting the disclosure of tax-related data solely for tax collection purposes—even preventing access by courts.³¹⁷ Similarly, Dutch financial and competition regulators are prohibited from repurposing confidential information gathered in the course of their duties.³¹⁸ Luxembourg extends tax secrecy even further, applying it beyond customs authorities to all public bodies³¹⁹ and explicitly preventing the Competition Authority from accessing tax-protected information, whether from judicial authorities or domestic and

³¹⁶ Lannier, Tosza, (n. 5), p. 325.

³¹⁷ De Vries et al., (n. 1), p. 366.

³¹⁸ *Ibid.* pp. 366-367.

³¹⁹ Lannier, Tosza, (n. 5), p. 326.

foreign tax administrations.³²⁰ More generally, Luxembourg upholds official secrecy as a default rule across various sectors, including banking, financial markets, and competition.³²¹ By contrast, Finland takes a more flexible approach, allowing customs authorities to transfer information to the tax administration and police when necessary.³²² Similarly, Belgium has adopted a very flexible approach, allowing competition, financial institutions, data protection, and VAT authorities to share confidential information with other designated national administrative bodies.³²³ By transferring this information, the obligation of professional secrecy is also transferred.

Across jurisdictions, exceptions to official secrecy enabling data transfers are common, but their scope and legal clarity vary significantly. Some countries, like the Netherlands³²⁴ and Germany,³²⁵ adopt a more restrictive and formalised approach: data may only be shared when explicitly required by law or justified by necessity and proportionality, such as for criminal investigations or judicial cooperation. In contrast, France³²⁶ and Finland³²⁷ allow broader inter-agency data sharing, with France explicitly excluding secrecy obligations for certain authorities and Finland mandating cooperation with tax and financial regulators. Meanwhile, Italy³²⁸ and Belgium³²⁹ lack clear statutory rules and instead rely on Memorandums of Understanding to facilitate cooperation, reflecting a more ad hoc and potentially less transparent model.

Some jurisdictions impose stricter rules on data transfer, particularly by limiting the purposes for which transferred data may be used. In Belgium, cooperation in competition matters requires a formal agreement enshrined in a royal decree, such as with the Belgian Institute for Postal Services and Telecommunications.³³⁰ Finland also restricts the competition authority's ability to transfer data, permitting it only for judicial authorities, tax administration, and financial regulators, and even then, only within the narrow scope of electricity and natural gas supply supervision.³³¹ Luxembourg enforces strict purpose limitations in the financial sector,

³²⁰ *Ibid.* p. 331.

³²¹ *Ibid.* pp. 316, 320.

³²² Riekkinen, (n. 3), p. 159.

³²³ Franssen, Vandormael, (n. 6), pp. 94-95.

³²⁴ De Vries et al., (n. 1), pp. 366-367.

³²⁵ Blume et al., (n. 18), pp. 236, 329-340.

³²⁶ Lassalle, (n. 2), p. 194.

³²⁷ Riekkinen, (n. 3), p. 159.

³²⁸ Lasagni, (n. 17), pp. 287, 290.

³²⁹ Franssen, Vandormael, (n. 6), p. 94.

³³⁰ *Ibid.* p. 95.

³³¹ Riekkinen, (n. 3), p. 160.

prohibiting further use of transferred data unless explicit consent is obtained.³³²

Rules governing data transfers between administrative and criminal authorities vary widely across jurisdictions, reflecting different balances between enforcement efficiency and procedural safeguards. Some countries, like France³³³ and Luxembourg,³³⁴ impose a legal duty on administrative bodies to report suspected criminal offences and transfer relevant data to judicial authorities, ensuring systematic cooperation. Others, such as Finland³³⁵ and Ireland,³³⁶ adopt a more discretionary model, where reporting is optional or based on voluntary cooperation. Belgium presents a mixed approach: while VAT authorities routinely share data with prosecutors,³³⁷ other bodies like competition and data protection authorities rely on informal practices, often contingent on prosecutorial willingness.³³⁸ Germany and Italy take a more restrictive stance, requiring that data transfers meet specific legal thresholds—Germany limits transfers to cases involving distinct offences,³³⁹ while Italy mandates compliance with criminal procedure rules and evidentiary safeguards.³⁴⁰

The transfer of data from judicial to administrative authorities is permitted in all studied jurisdictions, but the conditions and safeguards vary considerably. Some countries, like the Netherlands and Italy, allow such transfers under strict procedural conditions: Dutch courts permit the use of criminal evidence in administrative proceedings if judicial oversight is ensured—a practice upheld by the ECtHR³⁴¹ but controversial among scholars—³⁴² while Italy requires compliance with the double-proportionality test established by the ECJ, despite lacking explicit national rules.³⁴³ France³⁴⁴ and Luxembourg adopt sector-specific approaches, granting prosecutors discretion to share data, though Luxembourg requires judicial authorisation when criminal investigations are ongoing.³⁴⁵ Germany applies

³³² Lannier, Tosza, (n. 5), p. 327.

³³³ Lassalle, (n. 2), p. 195.

³³⁴ Lannier, Tosza, (n. 5), p. 327.

³³⁵ Riekkinen, (n. 3), p. 159.

³³⁶ Ni Loideain, (n. 12), p. 264.

³³⁷ Franssen, Vandormael, (n. 6), p. 97.

³³⁸ *Ibid.* pp. 94, 97.

³³⁹ Blume et al., (n. 18), p. 239.

³⁴⁰ Lasagni, (n. 17), pp. 288-291.

³⁴¹ ECtHR, *Janssen de Jong Groep B.V. and Others v. the Netherlands*, 16.05.2023, no. 2800/16 (referred to the Grand Chamber); ECtHR, *Burando Holding B.V. and Port Invest B.V. v. the Netherlands*, 16.05.2023, no. 3124/16 and 3205/16.

³⁴² De Vries et al., (n. 1), pp. 368-370.

³⁴³ Lasagni, (n. 17), pp. 288.

³⁴⁴ Lassalle, (n. 2), p. 194.

³⁴⁵ Lannier, Tosza, (n. 5), p. 327.

consistent safeguards for both directions of data exchange, ensuring legal symmetry.³⁴⁶ In contrast, Finland and Belgium impose stricter controls: Finland mandates the destruction of surplus judicial data unless explicitly authorised for administrative use,³⁴⁷ and Belgium requires prior approval from judicial authorities for transfers involving ongoing criminal procedures.³⁴⁸

5.1.2. Transfer of evidence at international level

EU law offers many specific rules on administrative cooperation at supranational level.³⁴⁹ Overall, these legislative acts limit grounds for refusal when transferring data within the EU for administrative cooperation. However, at national level, rules on transfer of evidence at international level remain very diverse.

International data transfers by administrative authorities are governed by diverse national rules, reflecting varying levels of restrictiveness and legal clarity. Countries like the Netherlands³⁵⁰ and Germany³⁵¹ adopt a formal and cautious approach: transfers are only allowed to foreign authorities

³⁴⁶ Blume et al., (n. 18), p. 240.

³⁴⁷ Riekkinen, (n. 3), p. 161.

³⁴⁸ Franssen, Vandormael, (n. 6), p. 96.

³⁴⁹ See, for instance, Council Regulation (EC) no. 515/97 of 13.03.1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, Article 4; Regulation (EU) no. 952/2013 of the European Parliament and of the Council of 09.10.2013 laying down the Union Customs Code, Article 47; Regulation (EU) no. 596/2014 of the European Parliament and of the Council of 16.04.2014 on market abuse, Articles 25 and 26; Regulation (EU) 2016/1011 of the European Parliament and of the Council of 08.06.2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds, Article 39; Council Regulation (EC) no. 1/2003 of 16.12.2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, Article 12; GDPR, Article 61; Directive (EU) 2019/1 of the European Parliament and of the Council of 11.12.2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, Article 24; Directive (EU) 2016/680 of the European Parliament and of the Council of 27.04.2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, Article 50; Council Regulation (EU) no. 904/2010 of 07.10.2010 on administrative cooperation and combating fraud in the field of value added tax; Council Directive 2010/24/EU of 16.03.2010 concerning mutual assistance for the recovery of claims relating to taxes, duties and other measures; Council Directive 2011/16/EU of 15.02.2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EE.

³⁵⁰ De Vries et al., (n. 1), p. 370.

³⁵¹ Blume et al., (n. 18), p. 241.

performing comparable functions, often requiring explicit authorisation or court orders. Finland similarly limits transfers through a strict purpose limitation principle.³⁵² Luxembourg and France follow sector-specific models, with Luxembourg imposing stringent confidentiality and use restrictions—especially in financial and customs matters³⁵³—while France allows exchanges based on reciprocity and functional equivalence.³⁵⁴ Belgium permits broader sharing under competition law but faces practical constraints due to professional secrecy and procedural inconsistencies.³⁵⁵ At the other end of the spectrum, Ireland lacks a binding legal framework and relies on non-binding Memorandums of Understanding, offering flexibility but less legal certainty.³⁵⁶

5.2. The admissibility of data obtained from third parties

In most jurisdictions, there are no specific rules governing the admissibility of data obtained from third parties, meaning that general rules of evidence apply. Administrative proceedings across various countries generally follow the principle of free evaluation of evidence, according to which any information may be used as proof unless it is manifestly improper or obtained in violation of fundamental rights (NL,³⁵⁷ FR,³⁵⁸ GE,³⁵⁹ FI,³⁶⁰ BE,³⁶¹ LU³⁶², IT³⁶³, PL³⁶⁴). As literature and case law regarding admissibility of evidence gathered in administrative proceedings is limited, many countries refer to criminal procedure standards.

Admissibility of evidence in administrative proceedings is generally governed by broad principles, but national approaches differ in how strictly they apply safeguards. The Netherlands and Germany apply nuanced balancing tests: Dutch courts may exclude evidence that violates fundamental rights or lacks proportionality,³⁶⁵ while German courts assess whether the state's interest in prosecution outweighs individual rights and only admit transferred evidence if it could have been lawfully obtained in the receiving

³⁵² Riekkinen, (n. 3), p. 165.

³⁵³ Lannier, Tosza, (n. 5), p. 329.

³⁵⁴ Lassalle, (n. 2), pp. 175-176.

³⁵⁵ Franssen, Vandormael, (n. 6), p. 95.

³⁵⁶ Ni Loideain, (n. 12), p. 265.

³⁵⁷ De Vries et al., (n. 1), p. 372.

³⁵⁸ Lassalle, (n. 2), p. 196.

³⁵⁹ Blume et al., (n. 18), p. 241.

³⁶⁰ Riekkinen, (n. 3), p. 163.

³⁶¹ Franssen, Vandormael, (n. 6), p. 102.

³⁶² Lannier, Tosza, (n. 5), p. 331.

³⁶³ Lasagni, (n. 17), p. 292.

³⁶⁴ Kaszubowski, Steinborn, (n. 26), p. 394.

³⁶⁵ De Vries et al., (n. 1), pp. 349-351, 372.

proceeding.³⁶⁶ France, by contrast, exercises limited judicial scrutiny over admissibility.³⁶⁷ Finland and Belgium adopt stricter standards in administrative contexts, with Finnish authorities barred from using evidence that would be inadmissible on appeal,³⁶⁸ and Belgian regulators—especially in data protection and finance—applying cautious, criminal-law-inspired standards.³⁶⁹ Luxembourg and Italy take a more procedural approach: Luxembourg requires legal acquisition and proper communication,³⁷⁰ while Italian authorities assess admissibility case by case.³⁷¹

Sector-specific regulations may impose broad admissibility conditions. In Belgium, competition law explicitly allows various forms of evidence, such as documents, electronic messages, and recordings, but evidence is inadmissible if formal conditions are not met, reliability is compromised, or its use contravenes the right to a fair trial.³⁷² In contrast, rules on admissibility of evidence are not expressly provided by banking law, financial markets law, and data protection law, they apply, voluntarily, rules on criminal procedures by analogy.³⁷³ Similarly, Luxembourg's competition authority accepts a wide range of evidence, and information obtained is generally admissible unless controlled by specific procedural requirements, and the VAT authority admits evidence based on the records of its agents.³⁷⁴

When it comes to international data transfers, Dutch administrative authorities must verify that the foreign authority providing the data maintains an equivalent level of rights protection, ensuring compliance with fair trial principles.³⁷⁵ However, they are not required to verify the legality of how the data was obtained by the foreign authority, as this responsibility rests with the originating jurisdiction.³⁷⁶ Differently, the German Federal Court of Justice, in *Encrochat* decision, has further listed exhaustive reasons for declaring evidence inadmissible following an international transfer in criminal proceedings, which might be later transposed to administrative cooperation.³⁷⁷

³⁶⁶ Blume et al., (n. 18), p. 242.

³⁶⁷ Lassalle, (n. 2), p. 196.

³⁶⁸ Riekkinen, (n. 3), pp. 164-166.

³⁶⁹ Franssen, Vandormael, (n. 6), p. 102.

³⁷⁰ Lannier, Tosza, (n. 5), p. 331.

³⁷¹ Lasagni, (n. 17), p. 292.

³⁷² Franssen, Vandormael, (n. 6), p. 102.

³⁷³ *Ibid.* p. 103.

³⁷⁴ Lannier, Tosza, (n. 5), p. 331.

³⁷⁵ De Vries et al., (n. 1), 372.

³⁷⁶ *Ibid.* p. 374.

³⁷⁷ Blume et al., (n. 18), p. 243. The reasons are the following: violations of principles of international law, for instance, a violation of the sovereignty of another state; violations of the *ordre public*, especially of fundamental principles regarding the rule of law; violations of

6. CONCLUSIONS

The preceding analysis reveals a landscape where, despite the increasing digitisation of society, administrative authorities have so far demonstrated a limited appetite for gathering electronic evidence from third parties, particularly online service providers (OSPs), often preferring traditional gathering evidence from persons concerned by the investigation. However, this approach is beginning to evolve, with a growing recognition of the potential and necessity of leveraging electronic evidence in administrative enforcement across various jurisdictions.

The study revealed structural variations in administrative punitive enforcement, with some countries clearly separating administrative and criminal proceedings while others operate under dual systems or blended approaches. Furthermore, the lines between supervisory and investigative functions within administrative enforcement are often blurred. Importantly, there is a growing acknowledgement that many administrative punitive proceedings possess a ‘criminal nature’ under the jurisprudence of the ECtHR, necessitating the application of enhanced procedural safeguards.

The legislative frameworks governing administrative investigations present a contrast between comprehensive general laws and fragmented sector-specific regulations. Administrative authorities generally possess both specific and general powers to gather data from third parties, including OSPs, though the categories of addressees, the types of data accessible, and the conditions for requesting this information differ significantly across countries and sectors. What has been clearly demonstrated is that the laws offer abundant opportunities to request data from persons concerned, but those laws either do not apply or oftentimes it is unclear whether they apply to third parties (e.g., the OSPs). Their open formulation, however, on many occasions offer the possibility for them to be used to request data from third parties.

While foundational legal principles such as proportionality and the right to be heard underpin these proceedings, their specific application and protection vary. Notably, safeguards towards third parties subject to these data requests are limited and inconsistent, which can be explained by the fact that they are usually not written having in mind such data requests. This raises concerns about legal certainty and the protection of fundamental rights.

The transfer of data obtained through administrative investigation powers, both at national and international levels, relies mostly on general principles of cooperation and often varies significantly depending on the authorities and sectors concerned. Similarly, the admissibility of such data is

provisions of the law of mutual assistance that protect individual rights; violations of provisions of the constitution, especially an encroachment on fundamental rights; and violations of specific provisions in procedural law.

largely governed by the principle of free evaluation of evidence, with many jurisdictions drawing analogies from criminal procedure in the absence of specific administrative law precedents.

In conclusion, this research reveals that administrative punitive enforcement, at least in its legal framework and practice, seems to be less advanced in recognising the potential and need for electronic evidence, contrary to criminal enforcement.³⁷⁸ The research demonstrates that there is a noticeable lag in the comprehensive regulation of data access, particularly concerning information held by third parties in administrative proceedings, hence showing a need to adapt to the challenges of adapting to the digital age. The limited and inconsistent guarantees and remedies available to both third parties and the investigated person underscore the need for further reflection and the development of clearer legal standards at the crossroad of administrative and criminal law.

³⁷⁸ See a comprehensive analysis in V. Franssen, S. Tosza (eds.), *The Cambridge Handbook of Digital Evidence in Criminal* University Press, 2025.

14. POLICY RECOMMENDATIONS

S. TOSZA and S. LANNIER

1. INTRODUCTION

The ELEVADMIN project addresses a critical gap in the understanding of how electronic evidence can be gathered in administrative punitive investigations. While the use of such evidence has been extensively studied in the context of criminal law, administrative enforcement—particularly at the EU level and within Member States—has remained underexplored. The project investigates the legal bases, practical mechanisms, and institutional capacities for requesting electronic evidence from Online Service Providers (OSPs), with a particular focus on the role of the European Anti-Fraud Office (OLAF). It aims to assess the feasibility and implications of extending OLAF's powers in this domain, while ensuring compliance with fundamental rights and procedural safeguards.

The research undertook a comprehensive comparative analysis across nine EU Member States—Belgium, Finland, France, Germany, Ireland, Italy, Luxembourg, the Netherlands, and Poland—and at the EU level. It focused on five key areas of punitive administrative enforcement: customs, Value Added Tax (VAT), competition law, General Data Protection Regulation (GDPR) enforcement, and financial market supervision. These domains were selected for their relevance to the protection of the EU's financial interests and their varying degrees of interaction between administrative and criminal enforcement.

The comparative chapter reveals a fragmented and evolving legal landscape across nine EU Member States. While administrative authorities increasingly recognise the value of electronic evidence, particularly from OSPs, their powers to obtain such data remain inconsistent and often ambiguous. The study identifies a patchwork of specific and general legal bases, with significant variation in the scope of powers, categories of accessible data, procedural safeguards, and enforcement mechanisms. Notably, administrative frameworks often lack explicit procedural safeguards, prompting administrative courts to rely on overarching constitutional principles or general norms of administrative law to fill the gaps. The admissibility and transfer of electronic evidence—especially across

administrative and criminal domains—lack consistent specific standards, aside the general principle of the freedom of proof.

At EU level, the Directorate-General for Competition of the European Commission (DG COMP), the European Central Bank (ECB), and European Securities and Markets Authority (ESMA) possess extensive investigatory powers in their respective domains—competition law, banking supervision, and financial markets. Yet, there is a notable absence of explicit legal bases allowing them to request electronic evidence directly from OSPs. DG COMP and the ECB rely on broadly framed general powers to request any information (i.e., any kind of data), but their applicability to OSPs remains uncertain or limited by personal scope (e.g., ECB's powers are confined to supervised entities and their business partners). ESMA, by contrast, it is specifically allowed to request telephone and data traffic records, though, as for the ECB, only from supervised entities. Across all three authorities, the use of such powers in practice remains rare, with investigations typically relying on data obtained directly from the entities under investigation.

2. GENERAL RECOMMENDATIONS AS TO GATHERING OF ELECTRONIC EVIDENCE FROM OSPs IN PUNITIVE ADMINISTRATIVE PROCEEDINGS

These findings underscore the urgent need for clearer, more coherent legal frameworks to ensure effective, fundamental rights-compliant administrative enforcement in the digital age. First, a clear legal basis should be established—preferably at the EU level—to define when and how administrative authorities may access electronic evidence from third parties, particularly OSPs, including the types of data and applicable conditions. Second, procedural safeguards must be introduced for third parties, including to certain extent to the OSPs, by formalising data requests as administrative decisions and ensuring transparency, the right to be heard, and access to remedies. Third, intrusive data requests—especially those involving sensitive data—should be subject to prior authorisation by an independent or judicial authority, in line with European Court of Human Rights (ECtHR) and European Court of Justice (ECJ) case law, to uphold fundamental rights and ensure proportionality. Finally, the admissibility and transfer of electronic evidence between administrative and criminal proceedings must be clarified to prevent circumvention of safeguards and ensure legal coherence, particularly through the application of the purpose limitation principle.

Recommendation no. 1: Establish a Clear Legal Basis for Access to Electronic Evidence by Administrative Authorities

Many jurisdictions rely on general or ambiguously framed powers. A harmonised EU-level framework could define when and how administrative

authorities can request electronic evidence from OSPs, specifying the types of data (e.g., subscriber, traffic, content) and applicable conditions. In the absence of EU-level framework, Member States should ensure consistency among areas of enforcement, which could foster legal clarity around administrative investigations regimes. In particular, Member States could rely on EU definitions regarding typologies of OSPs and data, to ensure consistency between national and EU legislation. Also, Member States should clarify whether such a clear legal basis would be available under the supervision or investigation competences of administrative authorities, especially given that the distinction between these procedural stages remains blurred, or entirely absent, in many of the jurisdictions analysed.

Recommendation no. 2: Recognise Data Requests as Administrative Decisions with Procedural Safeguards

In many Member States, data requests issued by administrative authorities, particularly to third parties such as OSPs, are not formally recognised as administrative decisions. Instead, they are often treated as preliminary investigative steps, which results in the absence of procedural safeguards for both affected individuals and the addressees. This lack of formal recognition undermines transparency, legal certainty, and the protection of fundamental rights. To address this gap, legislation and judicial authorities should explicitly classify data requests as administrative acts or decisions. This would trigger the application, for the investigated person, of existing procedural safeguards, including the right to be notified (once it no longer jeopardises the investigation), the right to be heard, and access to effective remedies against data requests. While some safeguards may be inferred from general constitutional or administrative principles, most administrative frameworks lack detailed provisions governing the procedural aspects of data requests. These include provisions on the requirement of a reasoned decision, designation of the competent authority, notification procedures, and effective remedies. At a minimum, data requests should comply with the procedural guarantees enshrined in the GDPR.

Moreover, some safeguards should extend to third parties, such as OSPs, who are not the primary subjects of the investigation, but are instrumental for its execution. In many jurisdictions, OSPs can only challenge a data request once a sanction is imposed for non-compliance. However, such sanctions are not uniformly available across sectors, and where they exist, they vary significantly in scope and severity. This fragmented approach leaves OSPs without meaningful recourse in many cases, unless the OSP chooses to oppose the request and face a risk of a sanction. Such recognition is particularly important when the requested data may implicate the OSP itself, for example, in cases involving potential breaches of data protection, where

the principle against self-incrimination must be respected. To ensure proportionality and legality, third parties should be informed of the purpose and legal basis of the data request. This is particularly crucial when the data was originally retained for a specific purpose (e.g., investigation of serious crime), as the ECJ has repeatedly held that access to data must meet an equivalent threshold of seriousness (e.g., when it regards violations to administrative law or investigation of crimes by administrative authorities).¹

Finally, administrative and criminal investigative competences are often blurred or explicitly overlapping, particularly in systems where law enforcement authorities, whether administrative or criminal, can determine the most appropriate procedural route. This fluidity between enforcement regimes must not result in the erosion of criminal procedural safeguards. Therefore, it is essential to ensure that third parties, such as OSPs, have access to remedies to a similar degree as in criminal cases, especially when the investigation may ultimately lead to criminal proceedings.

Recommendation no. 3: Require Independent or Judicial Oversight for Intrusive Data Requests

To align with ECtHR and ECJ jurisprudence, particularly in cases involving data that may reveal ‘precise conclusions on the private lives of the persons’² (e.g., traffic or content data), requests should be subject to prior authorisation by a judicial or independent authority, especially when the data is not held by the investigated person. In particular, the scope of data requests must be clarified, as outlined in Recommendation no. 1, to ensure that data requiring judicial authorisation under criminal law is afforded equivalent protection in administrative proceedings. This is especially relevant in hybrid enforcement contexts, where administrative sanctions may qualify as criminal in nature under the ECtHR’s *Engel* criteria,³ or where administrative investigations may lead to or run parallel with criminal proceedings. Judicial or independent oversight serves as a critical safeguard to assess the necessity and proportionality of the measure, especially in light of the sensitivity of the data and the potential impact on fundamental rights, including the right to privacy, data protection, and due process. The principle of proportionality

¹ ECJ, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, 21.12.2016, C-203/15 and C-698/15, §115; ECJ, *A.G. v. Lietuvos Respublikos generalinė prokuratūra*, 07.09.2023, C-162/22, §43; ECJ, *La Quadrature du Net and Others v. Premier ministre and Ministère de la Culture*, 30.04.2024, C-470/21, §§95-122.

² ECJ, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 08.04.2014, C-293/12 and C-594/12.

³ ECtHR, *Engel and Others v. the Netherlands*, 08.06.1976, no. 48272/17, 57479/17, 510/18, 7936/18, 27115/18.

should guide the assessment of whether the purpose of the data request justifies the level of intrusion, ensuring that access to sensitive data is reserved for cases of sufficient gravity and legal clarity.

Recommendation no. 4: Clarify the Admissibility and Transfer of Evidence Between Proceedings

In the evolving landscape of EU enforcement, where administrative and criminal investigations increasingly intersect, the ability to transfer evidence, including electronic evidence, between proceedings is not merely a procedural convenience—it is a structural necessity. Rules should be adopted to regulate the transfer of evidence between administrative and criminal proceedings, ensuring that such transfers do not circumvent procedural safeguards and that evidence remains admissible under both frameworks. So far, much attention has been dedicated to international cooperation in the criminal justice system, on one side, and in administrative cooperation, on the other side. For instance, despite administrative sovereignty over taxation, the increasing mobility of taxpayers, the growth in cross-border transactions, as well as the internationalisation of financial instruments have led to develop in-depth administrative cooperation among their tax authorities through the cross-border framework and instruments provided at the EU level. Yet, little attention has been dedicated to the transfer of evidence gathered in administrative proceedings towards criminal proceedings.

In particular, Member States should apply the principle of purpose limitation when assessing the permissibility of transferring data gathered from third parties. This principle, rooted in ECJ case law on data retention and access, requires that data collected for one purpose, especially a serious one such as criminal investigation, should not be repurposed for a less serious objective, such as administrative violations. In legal systems where the boundaries between supervision, punitive administrative proceedings, and criminal investigations are often blurred or overlapping, the original purpose for which the data was collected must guide both the permissibility of its transfer (especially from criminal to administrative proceedings) and the procedural safeguards that should be triggered upon transfer (particularly from administrative to criminal proceedings). Ensuring that the seriousness of the investigative purpose aligns with the sensitivity of the data is essential to uphold the principle of proportionality and to protect fundamental rights.

3. GATHERING OF ELECTRONIC EVIDENCE FROM OSPs BY OLAF

While national and EU administrative authorities play a vital role in enforcing compliance and investigating irregularities, they face significant limitations in addressing the increasingly complex and transnational nature of

fraud affecting the EU budget. The digitalisation of illicit practices, the use of sophisticated concealment techniques, and the cross-border dimension of financial misconduct demand a coordinated and specialised response at the EU level. OLAF occupies a unique position in this landscape. It is tasked with protecting the financial interests of the EU through independent administrative investigations, particularly in contexts where national authorities lack jurisdiction, capacity, or incentive to act. OLAF's mandate is especially critical in cases involving internal EU institutions,⁴ non-participating Member States to the European Public Prosecutor's Office (EPPO),⁵ third countries,⁶ or when the EPPO declines to open an investigation.⁷ In these scenarios, OLAF serves as the EU's primary investigative body, and its effectiveness directly impacts the integrity of the EU budget. As fraud and irregularities evolve in tandem with digital technologies, OLAF must be equipped with tools that match the sophistication of the threats it faces.

OLAF's investigative powers have gradually expanded to reflect the changing nature of fraud and the growing importance of digital evidence. Recent reforms have introduced new capabilities, such as the power to request bank account information⁸ and to inspect privately owned devices used for professional purposes.⁹ These developments mark a shift toward investigative techniques traditionally associated with criminal proceedings, underscoring OLAF's need to operate in a fast-paced, technologically advanced environment. However, OLAF remains institutionally distinct from criminal law enforcement bodies like the EPPO. While the EPPO Regulation does not

⁴ Article 4 OLAF Regulation, Regulation (EU, Euratom) no. 883/2013 of the European Parliament and of the Council of 11.09.2013 concerning investigations conducted by the European Anti-Fraud Office.

⁵ The EPPO was established under enhanced cooperation. According to Article 86 Treaty on the Functioning of the EU, in the absence of unanimity in the Council, a group of at least nine Member States may establish enhanced cooperation on the basis of the draft regulation concerned. The EPPO Regulation was adopted in October 2017 by 22 out of 27 Member States. Currently, Hungary, Ireland and Denmark are not taking part in enhanced cooperation, while Poland and Sweden have recently decided to join. See Council Regulation (EU) 2017/1939 of 12.10.2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office.

⁶ Even if the EPPO has recently considered to be competent over criminal offences related to European Union funds allocated to third countries. Concretely and considering the seat of EU Institutions, bodies, offices and agencies (IBOAs) involved in expenditure, both Belgian and Luxembourgish criminal laws confirm that an offence is considered as having been committed on their territory whenever any constituent element of the criminal offence has taken place on their territory.

⁷ Article 12e OLAF Regulation and Article 101(3) EPPO Regulation.

⁸ Article 7(3) OLAF Regulation.

⁹ Article 3(5) and 4(2) OLAF Regulation.

explicitly address electronic evidence in general,¹⁰ European Delegated Prosecutors (EDPs) can rely on national criminal procedure laws to request such data.¹¹ OLAF, by contrast, lacks a comparable legal basis or practice for directly requesting electronic evidence from OSPs, placing it at a disadvantage in investigations in certain sectors that increasingly hinge on digital traces.

Despite its central role in safeguarding EU financial interests, OLAF currently does not possess the power to directly request electronic evidence—a gap that significantly undermines its investigative capacity. The ability to access subscriber data, traffic records, or content data held both by investigated persons and by third parties, including OSPs, is essential for uncovering hidden arrangements, identifying accomplices, and demonstrating the organised nature or intent behind fraudulent schemes. So far, OLAF has to rely on indirect and less straightforward mechanisms such as on-the-spot checks or general requests for information to obtain data from third parties. While OLAF's powers have evolved—particularly through the 2020 reform introducing a general duty of cooperation and enhanced procedural safeguards—its investigatory tools remain limited by the absence of coercive powers and enforceable mechanisms. Additionally, the fragmented nature of OLAF's legal framework, which combines EU regulations, internal guidelines, and national law, often results in legal uncertainty. Moreover, the admissibility of OLAF-collected evidence in national or EPPO proceedings depends on whether they act within their own framework under a complementary investigation or in support to an ongoing investigation at EPPO or national level. While in the latter OLAF must comply with the legal framework of the supported investigation, transfer of evidence following a complementary investigation raises challenges regarding compliance with national evidentiary standards and fundamental rights, and concerns about the effectiveness and legal robustness of OLAF's investigative outputs.

As digital evidence becomes indispensable in both administrative and criminal investigations, OLAF must be empowered to gather such data under clearly defined conditions and safeguards. The study underpinning this book highlights the feasibility of establishing a system analogous to OLAF's access to bank accounts, potentially supported by national anti-fraud coordination services and judicial oversight. Moreover, given OLAF's role in transmitting evidence to criminal authorities like the EPPO, and *vice versa*, it is crucial to regulate the admissibility and transfer of electronic evidence between

¹⁰ Council Regulation (EU) 2017/1939 of 12.10.2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office. Article 30(1)e however address interception of communications.

¹¹ Article 30(4) EPPO Regulation.

proceedings. Without such powers and frameworks, OLAF risks falling behind in the digital age, unable to meet the demands of modern fraud detection and enforcement.

4. RECOMMENDATIONS WITHIN THE CURRENT LEGISLATIVE FRAMEWORK OF OLAF

In the absence of legislative reform, OLAF can still enhance its operational effectiveness through the following measures:

Recommendation no. 5: Leverage National Legal Frameworks via Cooperation

OLAF should strengthen collaboration with national anti-fraud coordination services (AFCOS) to access electronic evidence indirectly, relying on national authorities' powers under domestic law. This would require formalised cooperation protocols and possibly judicial assistance at the national level. In particular, OLAF could seek judicial validation of especially intrusive data requests through national courts, thereby reinforcing the legitimacy and admissibility of such evidence in subsequent proceedings. However, OLAF may encounter difficulties in relying on national investigative powers, as administrative punitive frameworks vary significantly across sectors and Member States. Depending on the type of fraud or irregularity, national authorities may not possess equivalent powers to request electronic evidence, which limits OLAF's ability to access relevant data through cooperation mechanisms.

Recommendation no. 6: Develop Internal Guidelines for Voluntary Cooperation with OSPs

OLAF should establish a structured and transparent framework for requesting data from OSPs on a voluntary basis, particularly in the absence of a dedicated legal basis. Such a framework should promote consistency across investigations, ensure compliance with fundamental rights, and foster trust with private actors who may hold relevant electronic evidence. This approach should include standardised request templates, internal review procedures, technical protocols for secure data transfer, and safeguards for both investigated persons and third parties. These guidelines should be adopted pursuant to Article 17(8) of the OLAF Regulation, which empowers OLAF to develop internal rules governing its investigative practices. While non-binding, such guidelines would serve as a harmonising tool to guide OLAF's operational behaviour and signal its commitment to legal certainty and rights protection. They would also help clarify OLAF's expectations and

procedures for OSPs, encouraging cooperation in cases where formal powers are lacking.

In parallel, OLAF should continue to strengthen its technical capacity in digital investigations. This includes targeted training in open-source intelligence (OSINT), blockchain analytics, and metadata interpretation, as well as the development of internal expertise in emerging technologies. In doing so, OLAF should ensure that its practices align with the data protection framework, including the GDPR and the Artificial Intelligence Act.¹² This alignment is essential to ensure that voluntarily obtained data is handled lawfully, ethically, and in a manner that supports its admissibility in follow-up proceedings.

Recommendation no. 7: Enhance Evidence Transfer Mechanisms

The current fragmentation between administrative and criminal frameworks, particularly in the context of digital evidence, risks undermining both the effectiveness of investigations and the protection of fundamental rights. This is especially relevant for OLAF, whose administrative findings often serve as the basis for criminal prosecutions, notably by the EPPO. Given the close interconnection between OLAF's administrative investigations and subsequent criminal prosecutions, whether at the national level or through the EPPO, clarifying the rules governing evidence transfer is essential. Enhancing evidence transfer mechanisms is essential to ensure the operational continuity between OLAF and criminal enforcement bodies like the EPPO. OLAF should formalise procedures, such as through internal guidelines for the admissibility and transfer of electronic evidence between administrative and criminal proceedings, particularly with the EPPO. This includes ensuring compliance with the principle of purpose limitation and data protection rules. To that aim, guidelines should not only regard general legal principles but especially include technical rules around data transfer.

5. RECOMMENDATIONS TO AMEND THE LEGISLATIVE FRAMEWORK OF OLAF

While OLAF can already strengthen its operational framework through internal guidelines, particular attention must be given to embedding new investigatory powers within its formal legal mandate. The following recommendations are especially timely, as the European Commission is expected to publish its evaluation report on OLAF in June 2026. This report may serve as a basis for proposing amendments to the OLAF Regulation, including updates to its investigative powers to reflect the evolving nature of

¹² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13.06.2024 laying down harmonised rules on artificial intelligence.

fraud and irregularities affecting the EU's financial interests. Anticipating this reform process, it is essential to identify concrete legislative improvements that would enhance OLAF's ability to gather electronic evidence in a manner that is both effective and compliant with fundamental rights.

Recommendation no. 8: Introduce a Specific Legal Basis for Accessing Electronic Evidence from OSPs

OLAF's founding regulation should explicitly authorise the Office to request electronic evidence from OSPs, including subscriber, traffic, and content data, under clearly defined conditions. Such a reform should specify the categories of data OLAF may request, the circumstances under which such requests are justified, particularly under which proceedings, depending on the seriousness of the violation under investigation, and the procedural rights of data subjects and third parties, drawing on ECtHR and ECJ case law. In defining OSPs and data categories, the legal framework should refer to pre-existing EU definitions, to ensure consistency among sectors. In drafting such a specific legal basis, attention should be particularly drawn to consistency with the E-evidence Regulation.¹³

Recommendation no. 9: Define Procedural Safeguards and Oversight Mechanisms

Should this power be introduced, it would represent a significant expansion of OLAF's investigative reach into areas traditionally governed by criminal procedure. As such, it must be framed within a legal architecture that ensures compliance with the European Convention on Human Rights, the Charter of Fundamental Rights of the EU, and relevant case law of the ECtHR and the ECJ. In particular, requests for data should be classified as administrative decisions, thereby triggering procedural safeguards under EU and national administrative law for investigated persons. Data subjects, when appropriate, should be informed of the request and given an opportunity to contest it, unless secrecy is justified by the needs of the investigation. OSPs should be granted a minimum set of procedural safeguards, particularly in situations where data requests may implicate them directly or risk infringing the principle against self-incrimination. Minimal procedural safeguards are essential to ensure access to remedies and to uphold fundamental rights, especially in contexts where the boundaries between OLAF's administrative investigations and EPPO-led or national criminal proceedings are blurred.

¹³ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12.07.2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings.

Creating procedural protections for OSPs helps ensure that administrative processes do not inadvertently bypass the safeguards required in criminal investigations. For intrusive data types (e.g., traffic or content data), prior authorisation by a judicial or independent authority should be mandatory. Each request should be subject to a documented assessment of its necessity and proportionality, particularly in light of the fundamental rights at stake. Affected parties should have access to effective remedies, including the right to challenge the legality of the request and the use of the data obtained.

Recommendation no. 10: Enable Cross-Border Enforcement and Mutual Recognition

OLAF should be allowed to issue data access requests that are recognised across Member States, adapted for administrative investigations. As administrative punitive proceedings do not result in penalties as severe as those in criminal proceedings, such as deprivation of liberty, cross-border cooperation mechanisms in this domain should be designed with greater flexibility than those used under criminal cooperation frameworks. However, this flexibility must be balanced with appropriate safeguards, particularly given the diversity and overlap of competences between administrative and criminal enforcement at the EU level. In cases where an administrative investigation may lead to, or run parallel with, criminal proceedings, safeguards must be in place to ensure that the procedural rights applicable in criminal contexts are not undermined. This includes ensuring that data obtained through cross-border administrative cooperation is subject to adequate legal scrutiny and that its use in subsequent criminal proceedings respects the principles of legality, proportionality, and fundamental rights protection. More generally, provisions governing the transfer of electronic evidence between OLAF and national criminal authorities and the EPPO, should ensure that such transfers respect procedural safeguards and data protection principles.

ANNEX I QUESTIONNAIRE FOR NATIONAL RAPPORTEURS

Please describe the rules of gathering of electronic evidence for administrative punitive investigations in your legal system by answering the questions below. Please refer to existing legislation and caselaw. Please also mention if there are any efforts to amend the existing legislation. A crucial element of this research is the examination of the practice of using the identified legal frameworks as well as in general of gathering electronic evidence, which involves conducting interviews with representatives of the relevant authorities, stakeholders from the private sector and practitioners. This research concerns gathering of any type of data except financial data. It is focused on gathering that data from 3rd party private actors (as for instance, Internet service providers, financial institutions or any private actor with specific knowledge of an information system), so the expression “private actor” is used in that sense. The main private actors of interest for this research are different kinds of Internet service providers.

I. General question

1. Is there a general framework on punitive administrative proceedings in your legal system? If so, please describe its main features (if you describe those rules here, you may opt for only signalling the application of those rules below in section II-VI and limit your presentation to the relevant deviations from those rules). If there is no such general framework, please describe relevant particularities as regards punitive administrative proceedings in your legal system.

II. Customs enforcement

2. Which administrative authorities are competent to investigate and issue punitive administrative sanctions in the area of customs enforcement? What is the nature of their enforcement (administrative or mixed: criminal and administrative – please explain)?

3. What is the specific legal basis that these authorities have at their disposal, if any, to request electronic evidence from private actors?

Under this specific legal basis, please explain:

- a. Which private actors fall into the scope of these requests?
- b. What type of data may be requested?
- c. Under which conditions the data may be requested?
- d. What are the rules of transfer of data (deadlines, technical aspects etc.)?
- e. What are the sanctions and enforcement mechanisms applicable to those private actors for non-cooperation?
- f. What are the rules of ex-ante or ex-post authorisation or control of those requests?
- g. What are the rules protecting the interests of persons concerned by those requests and what are the remedies available to them?
- h. What are the remedies available to the private actors?
- i. What are the rules regarding foreign providers, territoriality and concerning conflicting legal obligations for non-national private actors?

>>> Please also explain the practice of the use of that legal basis.

4. Is there a general legal basis (e.g., a general obligation to provide information, a general production order) that may be used in order to request electronic evidence from private actors?

If, possible, please provided information as to:

- a. Which private actors fall into the scope of these requests?
- b. What type of data may be requested?
- c. Under which conditions the data may be requested?
- d. What are the rules of transfer of data (deadlines, technical aspects etc.)?
- e. What are the sanctions and enforcement mechanisms applicable to those private actors for non-cooperation?
- f. What are the rules of ex-ante or ex-post authorisation or control of those requests?
- g. What are the rules protecting the interests of persons concerned by those requests and what are the remedies available to them?
- h. What are the remedies available to the private actors?
- i. What are the rules regarding foreign providers, territoriality and concerning conflicting legal obligations for non-national private actors?

>>> Please also explain the practice of the use of that legal basis.

5. Is voluntary cooperation possible and used in practice to gather electronic evidence from private actors?

If yes:

a. What are the rules applicable to that type of cooperation (please – as far as possible – provide information enumerated under points a-h in the question above)?

b. Is thus obtained evidence admissible in the relevant proceeding?

III. Tax enforcement as regards VAT

6. Which administrative authorities are competent to investigate and issue punitive administrative sanctions in the area of tax enforcement as regards VAT? What is the nature of their enforcement (administrative or mixed: criminal and administrative – please explain)?

7. What is the specific legal basis that these authorities have at their disposal, if any, to request electronic evidence from private actors?

Under this specific legal basis, please explain:

a. Which private actors fall into the scope of these requests?

b. What type of data may be requested?

c. Under which conditions the data may be requested?

d. What are the rules of transfer of data (deadlines, technical aspects etc.)?

e. What are the sanctions and enforcement mechanisms applicable to those private actors for non-cooperation?

f. What are the rules of ex-ante or ex-post authorisation or control of those requests?

g. What are the rules protecting the interests of persons concerned by those requests and what are the remedies available to them?

h. What are the remedies available to the private actors?

i. What are the rules regarding foreign providers, territoriality and concerning conflicting legal obligations for non-national private actors?

>>> Please also explain the practice of the use of that legal basis.

8. Is there a general legal basis (e.g., a general obligation to provide information, a general production order) that may be used in order to request electronic evidence from private actors?

If, possible, please provided information as to:

- a. Which private actors fall into the scope of these requests?
- b. What type of data may be requested?
- c. Under which conditions the data may be requested?
- d. What are the rules of transfer of data (deadlines, technical aspects etc.)?
- e. What are the sanctions and enforcement mechanisms applicable to those private actors for non-cooperation?
- f. What are the rules of ex-ante or ex-post authorisation or control of those requests?
- g. What are the rules protecting the interests of persons concerned by those requests and what are the remedies available to them?
- h. What are the remedies available to the private actors?
- i. What are the rules regarding foreign providers, territoriality and concerning conflicting legal obligations for non-national private actors?

>>> Please also explain the practice of the use of that legal basis.

9. Is voluntary cooperation possible and used in practice to gather electronic evidence from private actors?

If yes:

- a. What are the rules applicable to that type of cooperation (please – as far as possible – provide information enumerated under points a-h in the question above)?
- b. Is thus obtained evidence admissible in the relevant proceeding?

IV. Punitive enforcement in the area of banking and financial markets

10. Which administrative authorities are competent to investigate and issue punitive administrative sanctions in the area of banking and financial markets? What is the nature of their enforcement (administrative or mixed: criminal and administrative – please explain)?

11. What is the specific legal basis that these authorities have at their disposal, if any, to request electronic evidence from private actors?

Under this specific legal basis, please explain:

- a. Which private actors fall into the scope of these requests?
- b. What type of data may be requested?
- c. Under which conditions the data may be requested?
- d. What are the rules of transfer of data (deadlines, technical aspects etc.)?
- e. What are the sanctions and enforcement mechanisms applicable to those private actors for non-cooperation?
- f. What are the rules of ex-ante or ex-post authorisation or control of those requests?
- g. What are the rules protecting the interests of persons concerned by those requests and what are the remedies available to them?
- h. What are the remedies available to the private actors?
- i. What are the rules regarding foreign providers, territoriality and concerning conflicting legal obligations for non-national private actors?

>>> Please also explain the practice of the use of that legal basis.

12. Is there a general legal basis (e.g., a general obligation to provide information, a general production order) that may be used in order to request electronic evidence from private actors?

If, possible, please provided information as to:

- a. Which private actors fall into the scope of these requests?
- b. What type of data may be requested?
- c. Under which conditions the data may be requested?
- d. What are the rules of transfer of data (deadlines, technical aspects etc.)?
- e. What are the sanctions and enforcement mechanisms applicable to those private actors for non-cooperation?
- f. What are the rules of ex-ante or ex-post authorisation or control of those requests?
- g. What are the rules protecting the interests of persons concerned by those requests and what are the remedies available to them?

- h. What are the remedies available to the private actors?
- i. What are the rules regarding foreign providers, territoriality and concerning conflicting legal obligations for non-national private actors?

>>> Please also explain the practice of the use of that legal basis.

13. Is voluntary cooperation possible and used in practice to gather electronic evidence from private actors?

If yes:

- a. What are the rules applicable to that type of cooperation (please – as far as possible – provide information enumerated under points a-h in the question above)?
- b. Is thus obtained evidence admissible in the relevant proceeding?

V. Competition law enforcement

14. Which administrative authorities are competent to investigate and issue punitive administrative sanctions in the area of competition law enforcement? What is the nature of their enforcement (administrative or mixed: criminal and administrative – please explain)?

15. What is the specific legal basis that these authorities have at their disposal, if any, to request electronic evidence from private actors?

Under this specific legal basis, please explain:

- a. Which private actors fall into the scope of these requests?
- b. What type of data may be requested?
- c. Under which conditions the data may be requested?
- d. What are the rules of transfer of data (deadlines, technical aspects etc.)?
- e. What are the sanctions and enforcement mechanisms applicable to those private actors for non-cooperation?
- f. What are the rules of ex-ante or ex-post authorisation or control of those requests?
- g. What are the rules protecting the interests of persons concerned by those requests and what are the remedies available to them?
- h. What are the remedies available to the private actors?

i.What are the rules regarding foreign providers, territoriality and concerning conflicting legal obligations for non-national private actors?

>>> Please also explain the practice of the use of that legal basis.

16. Is there a general legal basis (e.g., a general obligation to provide information, a general production order) that may be used in order to request electronic evidence from private actors?

If, possible, please provided information as to:

- a. Which private actors fall into the scope of these requests?
- b. What type of data may be requested?
- c. Under which conditions the data may be requested?
- d. What are the rules of transfer of data (deadlines, technical aspects etc.)?
- e. What are the sanctions and enforcement mechanisms applicable to those private actors for non-cooperation?
- f.What are the rules of ex-ante or ex-post authorisation or control of those requests?
- g. What are the rules protecting the interests of persons concerned by those requests and what are the remedies available to them?
- h. What are the remedies available to the private actors?
- i.What are the rules regarding foreign providers, territoriality and concerning conflicting legal obligations for non-national private actors?

>>> Please also explain the practice of the use of that legal basis.

17. Is voluntary cooperation possible and used in practice to gather electronic evidence from private actors?

If yes:

- a. What are the rules applicable to that type of cooperation (please – as far as possible – provide information enumerated under points a-h in the question above)?
- b. Is thus obtained evidence admissible in the relevant proceeding?

VI. GDPR enforcement

18. Which administrative authorities are competent to investigate and issue punitive administrative sanctions in the area of GDPR enforcement? What is the nature of their enforcement (administrative or mixed: criminal and administrative – please explain)?

19. What is the specific legal basis that these authorities have at their disposal, if any, to request electronic evidence from private actors?

Under this specific legal basis, please explain:

- a. Which private actors fall into the scope of these requests?
- b. What type of data may be requested?
- c. Under which conditions the data may be requested?
- d. What are the rules of transfer of data (deadlines, technical aspects etc.)?
- e. What are the sanctions and enforcement mechanisms applicable to those private actors for non-cooperation?
- f. What are the rules of ex-ante or ex-post authorisation or control of those requests?
- g. What are the rules protecting the interests of persons concerned by those requests and what are the remedies available to them?
- h. What are the remedies available to the private actors?
- i. What are the rules regarding foreign providers, territoriality and concerning conflicting legal obligations for non-national private actors?

>>> Please also explain the practice of the use of that legal basis.

20. Is there a general legal basis (e.g., a general obligation to provide information, a general production order) that may be used in order to request electronic evidence from private actors?

If, possible, please provided information as to:

- a. Which private actors fall into the scope of these requests?
- b. What type of data may be requested?
- c. Under which conditions the data may be requested?
- d. What are the rules of transfer of data (deadlines, technical aspects etc.)?

- e. What are the sanctions and enforcement mechanisms applicable to those private actors for non-cooperation?
- f. What are the rules of ex-ante or ex-post authorisation or control of those requests?
- g. What are the rules protecting the interests of persons concerned by those requests and what are the remedies available to them?
- h. What are the remedies available to the private actors?
- i. What are the rules regarding foreign providers, territoriality and concerning conflicting legal obligations for non-national private actors?

>>> Please also explain the practice of the use of that legal basis.

21. Is voluntary cooperation possible and used in practice to gather electronic evidence from private actors?

If yes:

- a. What are the rules applicable to that type of cooperation (please – as far as possible – provide information enumerated under points a-h in the question above)?
- b. Is thus obtained evidence admissible in the relevant proceeding?

VII. Transfer of evidence between proceedings

- 22. What are the relevant rules on the transfer of evidence from an administrative to another administrative proceeding?
- 23. What are the relevant rules on the transfer of evidence from a criminal to an administrative proceeding?
- 24. What are the relevant rules on the transfer of evidence from an administrative to a criminal proceeding?
- 25. What are the relevant rules on the transfer of evidence from a foreign administrative proceeding to an administrative proceeding in your country?
- 26. What are the relevant rules on the transfer of evidence from a foreign criminal proceeding to an administrative proceeding in your country?
- 27. What are the relevant rules on the transfer of evidence from a foreign administrative proceeding to a criminal proceeding in your country?
- 28. Please explain – unless you have already done it in questions 22-27 – the relevant rules of admissibility of evidence in the above scenarios.

DETAILED TABLE OF CONTENTS

Table of contents	III
List of authors.....	V
List of abbreviations and acronyms	XV

1. SHEDDING LIGHT: ELECTRONIC EVIDENCE IN ADMINISTRATIVE INVESTIGATIONS	1
1. Introduction	1
2. Electronic evidence: from criminal to punitive administrative proceedings.....	2
2.1. Towards the E-evidence Regulation.....	2
2.2. The gap around administrative law enforcement	4
2.2.1. Gathering electronic evidence for administrative enforcement authorities	5
2.2.2. Regulating investigations in a world of interconnected law enforcement authorities	6
2.3. Perspective from the Council of Europe and the European Court of Human Rights	8
3. Methodology of this research	9
3.1. Selected areas of enforcement.....	9
3.2. A comparative analysis.....	10
3.3. A ‘law in action’ analysis	11
4. The structure of the book.....	11

2. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN THE EU 13

1. Competent authorities in selected areas of punitive administrative enforcement	13
1.1. DG COMP	13
1.2. ECB	16
1.3. ESMA	19
1.4. Customs enforcement	21
1.5. Tax enforcement as regards VAT	22
1.6. GDPR enforcement	23
2. Punitive administrative proceedings: general framework	24
3. Punitive administrative proceedings: sectorial framework	26
3.1. Requests for data to online service providers	26
3.1.1. Competition law enforcement	26
3.1.2. Punitive enforcement in the area of banking law and financial markets	34
3.1.2.1. ECB	34
3.1.2.2. ESMA	36
3.1.3. Customs enforcement	41
3.1.4. Tax enforcement as regards VAT	41
3.1.5. GDPR enforcement	43
4. Transfer of data between proceedings	45
4.1. Transfers of data between EU and national proceedings	45
4.1.1. Customs enforcement	46
4.1.2. Tax enforcement as regards VAT	46
4.1.3. Punitive enforcement in the area of banking law and financial markets	49
4.1.3.1. ECB	49
4.1.3.2. ESMA	51
4.1.4. Competition law enforcement	52
4.1.5. GDPR enforcement	54
4.2. Admissibility of data collected from online service providers as evidence	56
5. Conclusion	59

3. GATHERING OF ELECTRONIC EVIDENCE FOR THE PROTECTION OF THE FINANCIAL INTERESTS OF THE EU 63

1. The European Anti-Fraud Office (OLAF)	63
2. Punitive administrative proceedings: General Legal Framework	66
3. Punitive administrative proceedings: OLAF's Legal framework	67
3.1. Requests for data to online service providers	67
3.1.1. On-the-spot check and inspections	68

3.1.2. Requests for information.....	71
3.2. Procedural guarantees	72
3.2.1. Procedural rights	72
3.2.2. Remedies	75
4. Transfer of data between proceedings	79
4.1. Transfer of information before the opening of an investigation	79
4.2. Transfer of evidence during an investigation	79
4.3. Transfer of information upon completion of an investigation	81
4.4. Admissibility of data collected from online service providers as evidence.....	83
5. Conclusion.....	84

4. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN BELGIUM..... 87

1. Introduction	87
2. Administrative authorities in selected areas of punitive enforcement.....	89
3. Punitive administrative proceedings: lack of general framework, tentative categorisation.....	92
4. Punitive administrative proceedings: sectorial framework	94
4.1. Introduction	94
4.2. Requests for evidence to OSPs (and other private actors as third parties).....	96
4.2.1. Customs enforcement.....	96
4.2.2. Tax enforcement as regards VAT.....	98
4.2.3. Punitive enforcement in the area of financial markets law	100
4.2.4. Punitive enforcement in the area of banking law	102
4.2.5. Competition law enforcement	103
4.2.6. Data protection law enforcement	104
4.3. Voluntary cooperation	106
4.4. Concluding remarks	107
5. Transfer of evidence between proceedings	108
5.1. Transfers of evidence between national proceedings.....	108
5.1.1. Transfer of information between administrative authorities	108
5.1.2. Transfer of information between administrative authorities and the public prosecutor's office	113
5.1.2.1. Introduction	113
5.1.2.2. Taking the public prosecutor's office perspective.....	114
5.1.2.3. Similar rules for exchange of information with administrative and judicial authorities... ..	114
5.1.2.4. Yet, special rules regarding the notification of offences and to conditions for switching to criminal enforcement.....	115

5.1.2.5. Separate rules for the cooperation with the public prosecutor	118
5.1.2.6. Lack of formal rules	119
5.2. Transfers of evidence between foreign and national proceedings...	120
5.2.1. Introduction	120
5.2.2. National rules and practices	120
5.3. Admissibility of evidence.....	123
6. Conclusion.....	128
Annex 1 – List of interviews	129

5. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN FINLAND..... 131

1. Competent authorities in selected areas of punitive administrative enforcement	131
2. Punitive administrative proceedings: general framework	136
3. Punitive administrative proceedings: sectorial framework	142
3.1. Requests for data to online service providers	142
3.1.1. Customs enforcement	142
3.1.2. Tax enforcement as regards VAT	144
3.1.3. Punitive enforcement in the area of banking law and financial markets	148
3.1.4. Competition law enforcement	152
3.1.5. GDPR enforcement	157
3.2. Voluntary cooperation	161
4. Transfer of data between proceedings	162
4.1. Transfers of data between national proceedings	162
4.2. Transfers of data between foreign and national proceedings	166
4.3. Admissibility of data collected from online service providers as evidence.....	167
5. Conclusion.....	170

6. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN FRANCE..... 175

1. Competent authorities in selected areas of punitive administrative enforcement	175
2. Punitive administrative proceedings: general framework	176
3. Punitive administrative proceedings: sectorial framework	180
3.1. Specific requests for data to online service providers.....	180
3.1.1. Customs enforcement	180
3.1.2. Tax enforcement as regards VAT	182

3.1.3. Punitive enforcement in the area of banking law and financial markets	185
3.1.4. Competition law enforcement	187
3.1.5. GDPR enforcement	189
3.2. General production orders and search and seizure powers	189
3.2.1. Customs enforcement	189
3.2.2. Tax enforcement as regards VAT	190
3.2.3. Punitive enforcement in the area of banking law and financial markets	192
3.2.4. Competition law enforcement	192
3.2.5. GDPR enforcement	195
3.3. Requests to online service providers: the bigger picture.....	196
4. Transfer of data between proceedings	198
4.1. Transfers of data between national proceedings	198
4.2. Transfers of data between foreign and national proceedings	200
4.3. Admissibility of data collected from online service providers as evidence.....	201
5. Conclusion.....	202
Annex - Table: Duration of data retention based on the nature of the information and on the purpose of data retention	204

7. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN GERMANY 207

1. Competent authorities in selected areas of punitive administrative enforcement.....	207
1.1. Competent authorities in customs enforcement	207
1.2. Competent authorities in tax enforcement as regards VAT	208
1.3. Competent authorities in punitive enforcement in the area of banking law and financial markets.....	209
1.4. Competent authorities in competition law enforcement	210
1.5. Competent authorities in GDPR enforcement.....	211
2. Punitive administrative proceedings: general framework.....	211
2.1. General remarks	211
2.1.1. Regulatory offences in German law	211
2.1.2. General framework for gathering evidence from third parties in regulatory offence proceedings	215
2.1.3. General characteristics of these requests.....	220
2.2. Specific request for data to online service providers: subscriber data request.....	222
2.2.1. Definition of OSP.....	222
2.2.2. Type of data or information that can be requested	223
2.2.3. Conditions to request data	224

2.2.4. Rules on the transfer of data.....	226
2.2.5. Sanctions and enforcement mechanisms.....	227
2.2.6. Remedies for the concerned person	228
2.2.7. Remedies for the OSP	228
2.2.8. Rules regarding foreign providers, territoriality and concerning conflicting legal obligations	229
2.3. General requests for information to private third parties	229
2.3.1. Obligation to surrender (§ 46 OWiG in conjunction with §§ 94, 95 StPO)	229
2.3.2. General investigative clause (§ 46 (2) OWiG in conjunction with §§ 161, 163 StPO)	231
3. Punitive administrative proceedings: sectorial framework	232
3.1. Requests for data to online service providers	232
3.1.1. Customs enforcement.....	232
3.1.2. Tax enforcement as regards VAT.....	232
3.1.3. Punitive enforcement in the area of banking law and financial markets	233
3.1.4. Competition law enforcement	235
3.1.5. GDPR enforcement	240
3.2. Voluntary cooperation	242
4. Transfer of data between proceedings	244
4.1. Transfers of data between national proceedings	244
4.2. Transfers of data between foreign and national proceedings	246
4.3. Admissibility of data collected from online service providers as evidence.....	247
5. Conclusion.....	250

8. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE

ADMINISTRATIVE PROCEEDINGS IN IRELAND..... 251

1. Introduction	251
2. Punitive administrative proceedings: a common law approach	253
2.1. The Irish Constitution and the ‘administration of justice’	253
2.2. <i>Zalewski</i> : ‘fair procedures’ for investigated persons and administrative sanctions	255
2.3. <i>Zalewski</i> : implications for OSPs as third parties in administrative proceedings.....	257
3. Competent authorities in selected areas of punitive administrative enforcement.....	258
3.1. Digital Regulators Group (DRG)	258
3.1.1. Competition and Consumer Protection Commission (CCPC)	259
3.1.2. Data Protection Commissioner (DPC)	259
3.2. Other competent authorities	260

3.2.1. Central Bank of Ireland (CBI) (Banking and Financial Services)	260
3.2.2. Office of the Revenue Commissioners (VAT Enforcement)	261
4. Punitive administrative proceedings: sectoral approaches	262
4.1. Requests for data: voluntary cooperation from OSPs by default	262
4.2. Enforcement by Digital Regulators Group (DRG)	263
4.2.1. GDPR enforcement	263
4.2.2. Competition law enforcement	264
4.3. Enforcement in Banking (Central Bank of Ireland) (CBI).....	265
4.4. Enforcement in VAT (Revenue Office)	268
5. Transfer of data between proceedings	269
5.1. Transfers of data between national proceedings and authorities	269
5.2. Transfers of data between foreign and national proceedings	270
5.3. Admissibility of data collected from OSPs as third parties as evidence.....	271
6. Conclusion.....	271

9. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN ITALY..... 273

1. Competent authorities in selected areas of punitive administrative enforcement	273
2. Punitive administrative proceedings: sectoral framework	278
2.1. Requests for data to OSPs	278
2.1.1. Financial market law	278
2.1.2. Competition law	281
2.2. General investigatory powers to collect information	284
2.2.1. Customs enforcement	284
2.2.2. Tax enforcement as regards VAT	286
2.2.3. Punitive enforcement in the area of banking law and financial markets	288
2.2.4. GDPR enforcement	290
3. Transfer of data between proceedings	291
3.1. Transfers of data between national proceedings	292
3.2. Transfers of data between foreign and national proceedings	298
4. Conclusion.....	298

10. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN LUXEMBOURG..... 301

1. Competent authorities in selected areas of punitive administrative enforcement	301
2. Punitive administrative proceedings: general framework	304

2.1. Framework on non-contentious administrative procedure.....	305
2.2. General principles of administrative law	307
3. Punitive administrative proceedings: sectoral framework	308
3.1. Requests for data to online service providers	308
3.1.1. Customs enforcement.....	308
3.1.2. Tax enforcement as regards VAT.....	309
3.1.3. Punitive enforcement in the area of banking law and financial markets	312
3.1.3.1. Requests for electronic information	314
3.1.3.2. Requests for information.....	315
3.1.3.3. Common rules	318
3.1.4. Competition law enforcement	324
3.1.5. GDPR enforcement	326
3.2. Administrative requests to online service providers: the bigger picture.....	328
4. Transfer of data between proceedings	331
4.1. Transfers of data between national proceedings	331
4.2. Transfers of data between foreign and national proceedings	333
4.3. Admissibility of data collected from online service providers as evidence.....	336
5. Conclusion.....	338

11. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN THE NETHERLANDS 341

1. Competent authorities in selected areas of punitive administrative enforcement	341
1.1. Customs and tax (VAT) enforcement	342
1.2. Enforcement in the area of financial markets	342
1.3. Competition law enforcement	343
1.4. GDPR enforcement	344
2. Punitive administrative proceedings: general framework.....	345
2.1. Administrative sanctions under Dutch law, particularly the administrative fine.....	345
2.2. Competences to gather data as evidence under Dutch administrative law	347
2.2.1. The supervisory powers in the General Administrative Law Act	347
2.2.2. Questions on the gathering of digital evidence in accordance with administrative law	350
2.2.3. Intrusive investigative powers and Dutch criminal proceedings.....	352
2.3. Defence rights under Dutch administrative law	353

2.3.1. Legal professional privilege	353
2.3.2. Right to silence and privilege against self-incrimination.....	354
2.4. Legal protection against the gathering of data by Dutch administrative authorities	355
2.4.1. Legal protection before Dutch administrative (including tax) courts	356
2.4.2. Legal protection before Dutch civil courts.....	359
3. Punitive administrative proceedings: sectorial framework	360
3.1. Requests for data to online service providers	360
3.1.1. Customs and tax (VAT) enforcement	360
3.1.2. Punitive enforcement in the area of banking law and financial markets	363
3.1.3. Competition law enforcement	365
3.1.4. GDPR enforcement	370
4. Transfer of data between proceedings.....	373
4.1. Transfers of data between national proceedings	373
4.1.1. Sharing of information from administrative proceedings	373
4.1.2. Sharing of evidence from criminal proceedings	376
4.2. Transfers of data between foreign and national proceedings	378
4.3. Admissibility of data collected from online service providers as evidence.....	379
4.3.1. Use of data as evidence in (punitive) administrative proceedings.....	379
4.3.2. Use of digital data as evidence in criminal proceedings	380
5. Conclusion.....	382

12. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN POLAND..... 385

1. Competent authorities in selected areas of punitive administrative enforcement	385
1.1. Customs authority	386
1.2. Tax enforcement as regards VAT.....	387
1.3. Punitive enforcement in the area of banking law and financial markets	388
1.4. Competition law enforcement	389
1.5. GDPR enforcement	390
2. Punitive administrative proceedings: general framework	390
3. Punitive administrative proceedings: sectorial framework	392
3.1. Requests for data to online service providers	392
3.1.1. Customs enforcement.....	392
3.1.2. Tax enforcement as regards VAT	393

3.1.3. Punitive enforcement in the area of banking law and financial markets	394
3.1.4. Competition law enforcement	394
3.1.5. GDPR enforcement	398
4. Transfer of data between proceedings	398
4.1. Transfers of data between national proceedings	398
4.2. Transfers of data between foreign and national proceedings	401
4.3. Admissibility of data collected from online service providers as evidence.....	402
5. Conclusion.....	403

13. GATHERING ELECTRONIC EVIDENCE IN ADMINISTRATIVE PROCEEDINGS: COMPARATIVE ANALYSIS OF LAW AND PRACTICE..... 405

1. Introduction	405
2. The structure of administrative punitive enforcement	408
2.1. Criminal, supervisory and punitive administrative proceedings	408
2.2. Legislative overview of administrative proceedings.....	411
3. The content of administrative investigation powers towards OSPs	414
3.1. Specific administrative powers to gather data.....	414
3.1.1. Categories of OSPs as addressees to specific powers to request data.....	414
3.1.2. Categories of data under specific powers.....	417
3.1.3. Conditions to request data from certain OSPs	418
3.2. General administrative powers to gather information.....	420
3.2.1. Categories of third parties as addressees to general powers to request information	421
3.2.2. Conditions to request information to third parties	425
3.2.3. Categories of data under general powers	426
3.3. Transfer of data and enforcement of orders	430
3.3.1. Data transfer	430
3.3.2. Enforcement of requests.....	432
4. Legal safeguards in administrative investigation proceedings.....	434
4.1. Safeguards available to third parties	435
4.1.1. Protection against self-incrimination	435
4.1.2. Notification and right to be heard	436
4.1.3. Remedies	437
4.2. Safeguards available to the investigated person.....	439
5. Transfer and admissibility of data obtained from administrative investigation powers.....	441
5.1. The transfer of data obtained from third parties.....	442
5.1.1. Transfer of evidence at national level	442
5.1.2. Transfer of evidence at international level	445

5.2. The admissibility of data obtained from third parties	446
6. Conclusions	448
14. POLICY RECOMMENDATIONS.....	451
1. Introduction	451
2. General recommendations as to gathering of electronic evidence from OSPs in punitive administrative proceedings.....	452
3. Gathering of electronic evidence from OSPs by OLAF	455
4. Recommendations within the current legislative framework of OLAF.	458
5. Recommendations to amend the legislative framework of OLAF.....	459
 Annex I Questionnaire for national rapporteurs.....	 462
Detailed table of contents	471