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 ENFORCEMENT[1]

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 1/2003[4] 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 101[7] and Article 102[8] 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 a 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 Regulation[26] 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. Allegrezza, 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 entity[30] – 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 2011on 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 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 Sanchez-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

[76]ECJ, *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 information[92] 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 Brekout 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, Universita 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 II[183] 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 primary 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 e 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 authority[226]

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 Members 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 possession[243] 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 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 proceeding 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'Eerdt, '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'Eerdt, '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, 'GPDR 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).
[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 safeguardeed 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 isnot 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 wasobtained 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. Szydlo, '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.