13. GATHERING ELECTRONIC EVIDENCE IN ADMINISTRATIVE PROCEEDINGS: COMPARATIVE ANALYSIS OF LAW AND PRACTICE

S. TOSZA, S. LANNIER and F. JUNG

1. INTRODUCTION

The ELEVADMIN project was launched to address a critical and underexplored issue: the gathering of electronic evidence from Online Service Providers (OSPs) in administrative punitive investigations. Although electronic evidence has been widely examined in the context of criminal investigations, its role in administrative enforcement, especially within EU institutions and Member States, remains insufficiently studied. This research project seeks to fill that gap by analysing the legal foundations, operational procedures, and institutional capacities for administrative authorities to obtain electronic evidence from OSPs. This chapter undertakes a detailed comparative analysis across nine EU Member States, Belgium, Finland, France, Germany, Ireland, Italy, Luxembourg, the Netherlands, and Poland. It focuses on five key domains of administrative punitive enforcement: customs, Value Added Tax (VAT), competition law, data protection, and financial market supervision. These areas were selected for their relevance to the protection of the EU's financial interests and their varying degrees of overlap between administrative and criminal enforcement mechanisms. The findings reveal a fragmented and evolving legal landscape. This chapter identifies a mosaic of legal provisions, with considerable variation in the scope of authority, types of data accessible, procedural safeguards, and enforcement tools. Crucially, existing frameworks tend to receive limited procedural guarantees. Moreover, the rules governing the admissibility and transfer of electronic evidence, especially between administrative and criminal proceedings, are inconsistent and largely undeveloped, relying primarily on the general principle of free evaluation of evidence.

Despite the growing digitalisation of society, administrative authorities across studied jurisdictions have shown limited interest in gathering electronic evidence from third parties, particularly OSPs. This limited engagement with OSPs may not solely reflect institutional inertia or lack of

awareness. Rather, it may be rooted in deeper structural issues, including the absence of clear or suitable legal frameworks enabling such requests, or the perceived irrelevance of OSP-held data in certain enforcement contexts. Depending on the sector, the nature of the investigation, and the types of data typically required, administrative authorities may find that traditional sources, such as records held by the investigated entity, remain more accessible or probative. In some cases, the legal basis for requesting data from third parties is either too vague or narrowly defined, discouraging authorities from pursuing digital evidence beyond conventional means. This chapter explores how these legal and practical constraints shape the appetite for electronic evidence across jurisdictions and sectors.

Historically, evidence collection has focused on physical or on-site methods, as seen in the Netherlands where the 1990s General Administrative Law Act.[1] Similarly, in France, authorities supervising financial institutions have found little utility in sourcing information from third parties, preferring direct engagement with supervised entities.[2] Finland mirrors this trend, with VAT enforcement occasionally employing broad interpretations for evidence gathering but lacking established practices or case law concerning third-party data collection.[3] Finnish competition authorities primarily rely on on-site inspections, given the legal obligation for suspected entities to cooperate.[4] Belgium and Luxembourg also lean towards on-site collection, with Luxembourg's VAT authorities seldomly requesting data from others than taxpayers[5] and Belgium's data protection authority collecting most evidence on-site.[6]

However, this approach is beginning to evolve. In the Netherlands, administrative bodies are seeking powers better suited to technological advancements, though practical use remains rare.[7] Finland has seen isolated instances where the data protection authority accessed subscriber data from telecom operators,[8] and there is increasing demand for access to traffic data by authorities supervising financial institutions.[9] France's legislative

[1] A. De Vries et al., 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in the Netherlands', in this book, p. 342.
[2] M. Lassalle, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in France', in this book, p. 180.
[3] J. Riekkinen, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in Finland', in this book, p. 142.
[4] *Ibid.* pp. 149, 152-153, 156.
[5] S. Lannier, S. Tosza, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in Luxembourg', in this book, p. 303.
[6] V. Franssen, M. Vandormael, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in Belgium', in this book, pp. 101-103.
[7] De Vries et al., (n. 1), pp. 343, 354.
[8] Riekkinen, (n. 3), p. 157.
[9] *Ibid.* p. 145.

framework is gradually adapting under EU influence to craft new powers to gather telecommunication data in administrative proceedings,[10] and Belgium's competition authority has recently gained the ability to collect metadata.[11] Similarly, Ireland's legislative framework has undergone significant evolution influenced by developments in European Union law, positioning the country as a central hub for the headquarters of various international OSPs.[12] These entities play a crucial role in the collection of digital evidence. However, a comprehensive general framework addressing this domain remains absent.[13]

In parallel, recent years have seen a growing trend of public-private partnerships in data collection and enforcement activities across various jurisdictions, particularly in areas such as competition law, financial oversight, and tax enforcement. In the Netherlands, authorities have engaged in cooperative ventures with private actors to combat serious organised crime, leveraging external expertise and data sources.[14] Similarly, in Finland, competition law has been interpreted to allow the Finnish Competition and Consumer Authority (FCCA) direct access to public tender data through a private service provider, while customs authorities routinely obtain information from both public and private databases.[15] Belgium has also embraced private sector collaboration in competition law enforcement, notably in the collection, processing, and analysis of electronic evidence obtained during on-site inspections.[16] In Italy, tax authorities have gone even further by utilising social media and private digital platforms to detect tax evasion. Through partnerships with private companies, Italian authorities have cross-referenced online content—such as influencer marketing activities and adult platform earnings—with declared incomes, uncovering discrepancies.[17]

These developments suggest a shifting landscape where administrative authorities are starting to recognise the potential and necessity of leveraging electronic evidence in enforcement activities. In the face of this shift, this chapter analyses the powers of administrative authorities in selected areas of enforcement to gather data from third parties.

---

[10] Lassalle, (n. 2), pp. 172-173.
[11] Franssen, Vandormael, (n. 6) p. 101.
[12] N. Ni Loideain, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in Ireland', in this book, p. 245.
[13] *Ibid.* p. 246.
[14] De Vries et al., (n. 1), p. 368.
[15] Riekkinen, (n. 3), p. 158.
[16] Franssen, Vandormael, (n. 6), p. 102.
[17] G. Lasagni, 'Gathering of Electronic Evidence in Punitive Administrative Proceedings in Italy', in this book, p. 280.

To guide the reader through this complex and evolving landscape, the chapter adopts a structure that mirrors the progression typically found in the national chapters of this volume. It begins by examining the general structure of administrative punitive enforcement, which frames how investigative powers are allocated and exercised. This sets the foundation for the subsequent analysis of powers to gather data from third parties, starting with 'specific powers' granted to administrative authorities to request electronic evidence specifically from OSPs, a growing and often contentious domain. This is followed by a discussion of 'general powers' to request information from any third parties more broadly, which are often more ambiguously framed yet equally relevant in practice. The chapter then turns to the conditions for requesting such data and the types of data that may be accessed, before exploring the transfer and enforcement mechanisms available when OSPs fail to comply. Finally, it addresses the legal safeguards available to both third parties, including OSPs, and investigated persons, as well as the admissibility and further use of data obtained in administrative proceedings.

2. THE STRUCTURE OF ADMINISTRATIVE PUNITIVE ENFORCEMENT

The structure of administrative punitive enforcement plays a crucial role in determining how regulatory authorities operate, the legal tools available to them, and the extent to which procedural safeguards are applied. As administrative sanctions increasingly serve functions traditionally reserved for criminal law, such as deterrence and punishment, many jurisdictions are grappling with the boundaries between supervisory, investigative, and punitive actions. This section examines the legal and institutional arrangements underpinning administrative enforcement across selected jurisdictions. It explores the classification of proceedings, the division of powers between administrative and criminal bodies, and the overarching legislative frameworks that shape how administrative authorities investigate and sanction regulatory breaches.

2.1. Criminal, supervisory and punitive administrative proceedings

Understanding the distinctions and overlaps between criminal, supervisory and punitive administrative proceedings is essential for analysing how different legal systems approach the enforcement of regulatory norms. While traditionally viewed as separate domains, many jurisdictions exhibit hybrid structures in which administrative authorities exercise powers with punitive or quasi-criminal effects. This sub-section explores how the studied legal orders define and organise these different proceedings, focusing on the allocation of investigative and enforcement powers, the interplay between

administrative and criminal mechanisms, and the general procedural safeguards triggered by punitive measures.

The distinction between criminal and administrative enforcement is fundamental to understanding how different jurisdictions approach regulatory compliance and sanctions. Criminal enforcement typically involves the prosecution of offences that are considered harmful to public order, leading to penalties such as imprisonment or criminal fines, and follows strict procedural safeguards. In contrast, administrative enforcement addresses regulatory breaches through sanctions like administrative fines or corrective measures, often with more flexible procedures. Germany clearly separates these two systems: criminal offences are subject to mandatory prosecution by criminal authorities, while regulatory offences fall under administrative enforcement guided by the principle of opportunity.[18] The Netherlands and Italy, however, employ a dual enforcement system where authorities may choose between administrative or criminal proceedings based on the nature of the offence.[19] Belgium blends these approaches, with enforcement mechanisms varying across sectors depending on specific legislation and practices.[20]

Within administrative enforcement itself, there is also a distinction between supervision and investigation. Supervisory activities are preventive and aim to ensure compliance through monitoring and guidance, while investigative actions are reactive, focusing on detecting and addressing potential violations. Germany exemplifies this separation, with banking law and financial markets law assigning supervision and investigation to different departments within supervisory authorities.[21] Conversely, the Netherlands, despite distinguishing between reparatory and punitive sanctions,[22] grants administrative authorities identical powers for supervision and investigation.[23] Luxembourg,[24] Finland,[25] and Poland,[26] for the latter particularly regarding financial supervision, make no clear distinction between these functions, allowing authorities to seamlessly transition from supervision to investigation. This blurred line is particularly relevant when administrative bodies have dedicated criminal units—such as customs

[18] P. Blume et al., 'Gathering of Electronic Evidence in Administrative Punitive Proceedings in Germany', in this book, p. 208
[19] De Vries et al., (n. 1), p. 333; Lasagni, (n. 17), p. 267.
[20] Franssen, Vandormael, (n. 6), p. 87.
[21] Blume et al., (n. 18), p. 229.
[22] De Vries et al., (n. 1), p. 337.
[23] *Ibid*. p. 338.
[24] See *infra* Section 3.2.
[25] Riekkinen, (n. 3), p. 136.
[26] K. Kaszubowski, S. Steinborn, 'Gathering of Electronic Evidence in Administrative Punitive Proceedings in Poland', in this book, p. 379.

enforcement agencies in Belgium,[27] Finland,[28] France,[29] Germany,[30] Italy,[31] Luxembourg,[32] and Poland,[33] and tax administrations in Belgium,[34] Italy[35], Germany,[36] the Netherlands[37] and Poland[38]—which are enabled to apply criminal procedural rules when necessary. This blurred line is also sensitive when authorities receive discretionary power to impose either an administrative fine or to transfer the evidence towards criminal proceedings (see Section 4.1.1).[39] This structural variation across jurisdictions significantly influences how evidence is gathered and how enforcement measures are implemented.

Although administrative enforcement proceedings are formally classified as administrative in nature, there is a growing recognition that many of these proceedings qualify as 'criminal in nature' under the case law of the European Court of Human Rights (ECtHR).[40] This classification hinges on the severity and purpose of the sanctions imposed, which often mirror criminal penalties in their punitive intent and impact. In the Netherlands, legal literature widely acknowledges that administrative fines may be considered criminal in nature due to their punitive and deterrent functions.[41] Similarly, in Finland, scholars recognise that punitive administrative proceedings must adhere to the same procedural safeguards and due process rights as criminal proceedings.[42] This is particularly evident in sectors prone to economic misconduct, where administrative sanctions act as substitutes for criminal punishment.[43] Luxembourg also reflects this trend, with legal scholarship identifying sanctions imposed by financial sector[44] and data protection[45] authorities as criminal in nature. Belgium reflects a comparable trend, notably in competition law, where the Market Court, acknowledging the criminal

[27] Franssen, Vandormael, (n. 6), p. 85.
[28] Riekkinen, (n. 3), p. 127.
[29] Lassalle, (n. 2), p. 170.
[30] Blume et al., (n. 18), p. 202.
[31] Lasagni, (n. 17), p. 268.
[32] Lannier, Tosza, (n. 5), p. 194.
[33] Kaszubowski, Steinborn, (n. 26), p. 378.
[34] Franssen, Vandormael, (n. 6), p. 89.
[35] Lasagni, (n. 17), pp. 269-270.
[36] Blume et al., (n. 18), p. 202.
[37] De Vries et al., (n. 1), p. 334.
[38] Kaszubowski, Steinborn, (n. 26), p. 378.
[39] *Ibid.* p. 379.
[40] S. Tosza, S. Lannier, M. Siclari, 'Bridging the Gap: Electronic Evidence in Administrative Investigations', in this book, p. 1 ff.
[41] De Vries et al., (n. 1), p. 338.
[42] Riekkinen, (n. 3), p. 133.
[43] *Ibid.* p. 132.
[44] Lannier, Tosza, (n. 5), p. 296.
[45] *Ibid.* p. 297.

nature of administrative sanctions, provides full judicial oversight.[46] The Belgian Competition Authority has explicitly accepted that its sanctions carry a criminal character,[47] and in 2023, sanctions in the financial markets sector were officially recognised as criminal in nature under the European Convention on Human Rights (ECHR).[48] In Italy, the Italian Supreme Court and Constitutional Court have similarly recognised the criminal nature of sanctions imposed by the banking, financial markets and competition supervisors.[49] The latter authority may explicitly impose 'punitive sanctions', although such a category is not defined.[50] Comparably, in Ireland, following the *Zalewski* judgment, administrative entities may perform acts that are criminal in nature but must respect the law and principles of fair procedure. This includes investigative powers that may affect fundamental rights, for example regarding witnesses, as highlighted in the Irish case law referring to the ECtHR case law.[51] Germany differentiates between criminal and regulatory offences based on the sanction's nature, with the Federal Constitutional Court distinguishing criminal offences as carrying 'socio-ethical or dishonourable unworthiness', whereas regulatory fines are viewed as 'disobedience to the administration'.[52] Nonetheless, Germany's Act on International Mutual Assistance in Criminal Matters extends to regulatory offences, underscoring their quasi-criminal character.[53] This evolving perspective across jurisdictions necessitates the application of enhanced procedural safeguards—to ensure compliance with ECHR standards and to protect individuals from disproportionate state action in administrative enforcement proceedings.

2.2. Legislative overview of administrative proceedings

The legislative foundations of administrative enforcement differ markedly across jurisdictions, reflecting varying legal traditions, institutional structures, and approaches to administrative proceedings. While some countries rely on comprehensive and codified administrative procedure acts, others primarily regulate administrative proceedings through fragmented, sector-specific statutes. These divergences influence not only the coherence and accessibility of the legal framework but also the scope of investigative powers, the availability of procedural safeguards, and the consistency of

[46] Franssen, Vandormael, (n. 6), p. 88.
[47] *Ibid.*
[48] *Ibid*. p. 87.
[49] Lasagni, (n. 17), p. 284.
[50] *Ibid.* pp. 270-271.
[51] Ni Loideain, (n. 12), p. 251.
[52] Blume et al., (n. 18), pp. 205-207.
[53] *Ibid.* p. 240.

enforcement practices. This comparative overview of the legislative regimes governing administrative proceedings also explores the role of general principles of administrative law, and the implications for gathering electronic evidence from third parties.

The legislative structure governing administrative enforcement and investigation powers across the studied countries reveals a contrast between comprehensive general frameworks and fragmented sector-specific regulations. Germany exemplifies a more structured approach through the Act on Regulatory Offences, which governs administrative sanctions but refers to the Criminal Procedure Code for procedural matters, with necessary adaptations and explicit exclusions—for instance, limiting criminal investigative powers to a defined list of offences.[54] Finland adopts a similar general framework with its Administrative Procedure Act, applicable to all administrative matters, including investigations and punitive sanctions.[55] The Netherlands relies on the General Administrative Law Act of 1994, which standardises administrative procedures but notably excludes customs and tax matters, leaving these areas governed by separate legal frameworks.[56] Luxembourg operates under the 1978 Law on Non-Contentious Administrative Procedure and the 1979 Grand-Ducal Regulation, although their applicability to VAT enforcement remains ambiguous and these frameworks remain barely detailed.[57] Similarly, Italy[58] and Poland[59] rely on general administrative law on proceedings, which contains only general minimum rules. However, in all cases, these frameworks must be supplemented by sector-specific legislation detailing sanctions and procedural rules for particular sectors.

In contrast, France,[60] Belgium,[61] Italy[62] and Luxembourg lean heavily on sector-specific legislation, resulting in a fragmented and sometimes inconsistent legal framework. This is particularly evident in the financial sector, where Luxembourg has an array of over 15 distinct laws, each outlining supervisory powers with varying levels of detail and coherence.[63] Similar diversity can be found in the banking sector in Italy.[64] In Ireland, the fragmented legal framework results from the absence of codification in Irish

---

[54] *Ibid.* pp. 209-212.
[55] Riekkinen, (n. 3), p. 134.
[56] De Vries et al., (n. 1), p. 337.
[57] Lannier, Tosza, (n. 5), p. 301.
[58] Lasagni, (n. 17), p. 285.
[59] Kaszubowski, Steinborn, (n. 26), p. 380.
[60] Lassalle, (n. 2), p. 172.
[61] Franssen, Vandormael, (n. 6), p. 87.
[62] Lasagni, (n. 17), p. 267.
[63] Lannier, Tosza, (n. 5), p. 305.
[64] Lasagni, (n. 17), p. 268.

law.[65] However, the Irish Constitution establishes a foundation for investigating and enforcement powers in both administrative and criminal proceedings.[66] Recently, there has been a shift from a rigid judicial 'centralism' to a sector specific distribution of powers to administrative bodies.[67]

Generally, administrative punitive proceedings across the surveyed jurisdictions are governed by foundational legal principles designed to ensure fairness, legality, and the protection of fundamental rights. These principles, though not always codified, significantly influence administrative practices. Most jurisdictions refer to the principle of proportionality in administrative proceedings (NL, LU, GE, FI, IT, PL). Additionally, in the Netherlands, the principles of good administration, competence of the supervisory authority, and observance of fundamental rights guide proceedings.[68] Also, subsidiarity requires authorities to first seek information directly from the concerned party.[69] These general principles can be explicitly embedded in sectorial legislations, such as in Belgium, where the data protection authority must justify data requests by demonstrating proportionality and subsidiarity.[70] Luxembourg mandates that administrative authorities exercise decision-making powers impartially and act within a reasonable timeframe, and the country enshrines rights of defence and the adversarial principle under its Law governing non-contentious administrative procedures.[71] Germany integrates core criminal law principles such as the principle of legality, *lex mitior*, *in dubio pro reo*, the right to be heard, and the right to remain silent.[72] In Finland, constitutional guarantees underpin the legality of investigatory powers, necessitating precision in legal provisions and ensuring the right to an effective remedy, a fair trial, and good administration. Some general principles are differently protected under statutory law. Finnish law emphasises equal treatment, impartiality, and the right to be heard, requiring precise and timely communication in administrative procedures.[73] Similarly, Irish case law integrates the impartiality and independence of decision-makers as fundamental components of the good administration of justice.[74] .

[65] Ni Loideain, (n. 12), pp. 247, 252.
[66] *Ibid.* pp. 247-248.
[67] Franssen, Vandormael, (n. 6), p. 87.
[68] De Vries et al., (n. 1), p. 339.
[69] *Ibid.* p. 341.
[70] Franssen, Vandormael, (n. 6), p. 102.
[71] Lannier, Tosza, (n. 5), p. 300.
[72] Blume et al., (n. 18), p. 208.
[73] Riekkinen, (n. 3), pp. 133-134.
[74] Ni Loideain, (n. 12), p. 250.

3. THE CONTENT OF ADMINISTRATIVE INVESTIGATION POWERS TOWARDS OSPS

The growing reliance on OSPs as key data holders in administrative investigations has prompted a gradual expansion of investigatory powers across jurisdictions. This section provides a comparative overview of how these powers are structured and exercised, revealing a fragmented and often ambiguous legal landscape. While some authorities benefit from clearly defined, sector-specific powers to request data from OSPs ('specific powers'), others rely on broadly framed general powers whose applicability to OSPs is not always explicit ('general powers'). The analysis shows that the scope of powers, the categories of data accessible, and the conditions for requesting information vary significantly, often depending on the area of enforcement. Moreover, the distinction between specific and general powers is not always clear-cut in practice, and the legal frameworks frequently lack coherence or harmonisation. This section highlights the operational and normative challenges that arise when administrative authorities seek to access electronic evidence from actors who are not the primary subjects of investigation but are essential to its success.

3.1. Specific administrative powers to gather data

Specifically, some administrative authorities are granted powers, in some jurisdictions, to request data from OSPs. This section focuses on the categories of OSPs subject to such powers, the categories of data that may be accessed, and the legal and procedural conditions under which these powers may be exercised across jurisdictions. These powers are typically grounded in sector-specific legislation and are often shaped by EU law, though their scope and implementation vary significantly across the studied jurisdictions. The comparative analysis reveals that while some countries provide detailed and narrowly defined powers, clearly distinguishing between types of data and requiring strict conditions, others rely on broader or less clearly delimited frameworks. The categories of OSPs subject to these powers, the types of data that may be accessed and the conditions under which access is granted differ widely, with some authorities enjoying expansive reach and others facing legal or constitutional constraints. Overall, the section highlights a fragmented legal landscape which does not yet match the growing reliance on electronic evidence.

3.1.1. Categories of OSPs as addressees to specific powers to request data

In most countries (except in the Netherlands), administrative authorities are entitled to request data from certain types of third parties, including from OSPs. To delimit the addressees of these requests, some countries use, as in Poland,[75] or refer to definitions under EU law, although the transposition of these definitions are not always fully harmonised. Indeed, countries retain a certain margin of appreciation in transposing EU texts defining categorising OSPs. Certain legal cultures heavily rely on references to other frameworks, while other retain sectorial definitions and categories. Indeed, administrative proceedings frameworks do not always refer to national frameworks on electronic communications, leading to the multiplication of categories of OSPs and questioning the legal coherence among legal frameworks. Therefore, as in criminal law, definitions and categories of OSPs remain diverse at EU level.[76]

In Germany, all authorities can, under the general framework on regulatory offences investigation, specifically request subscriber data from providers of electronic communications service under the European Electronic Communications Code,[77] and from providers of digital services classified as Information Society services under the Information Society Services Directive.[78]

Most of the specific powers to gather data stem from sectorial legislation, although OSPs categories remain diverse even within one jurisdiction. For instance, Belgium's competition authority, since January 2023, may access data from electronic communications operators active on the Belgian market.[79] Similarly, Belgium's data protection authority may request data from electronic communication network operators within Belgian territory,[80] which categories derive from EU law. Finally, Belgium's financial markets supervisor may request metadata and identification data from operators of telecommunications networks and providers of a telecommunications service.[81]

---

[75] Kaszubowski, Steinborn, (n. 26), p. 382.

[76] V. Franssen, S. Tosza, 'A Comparative Analysis of National Law and Practices - Unravelling Differences in View of EU-Wide Solutions', *in*: V. Franssen, S. Tosza (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Matters*, Cambridge University Press, 2025, pp. 423-454.

[77] Article 2(4) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11.21.2018 establishing the European Electronic Communications Code.

[78] Blume et al., (n. 18), pp. 216-217. Article 1.1(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 09.09.2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

[79] Franssen, Vandormael, (n. 6), p. 102.

[80] *Ibid.*

[81] *Ibid.* p. 92.

France grants similar powers to gather telecommunication metadata to various authorities, including customs, VAT, financial market and competition supervisors. These powers cover electronic communications operators—defined as any entity operating a public electronic communications network or providing related services—and service providers offering online public communication services or hosting user-generated content.[82] In Ireland, the term OSP is broadly defined, encompassing a wide range of internet services, including *inter alia* webmail, messaging providers, hosting services, online marketplaces and search engines.[83]

In other countries, specific administrative powers to gather data are limited to the financial institution sectors. In Luxembourg, authorities in the financial institution sectors may request data from providers of electronic communication services and operators of public communication networks. Although those categories retain the wording of EU texts, Luxembourg's framework does not include, as under EU law, internet access or interpersonal communication services among electronic communications services.[84] Additionally, while some authorities may request telecommunications data from any entity, it remains unclear whether the power to issue such requests concerns only the entities under investigation or extends to other supervised entities acting as third-party OSPs, particularly in the data protection sector.[85] In Italy, administrative authorities may specifically request data only in the context of market abuse investigations, where the competent administrative authority may issue requests simply to anyone, or in certain context only to providers of the traffic data.[86] In Germany, supervisors in the financial institution sectors may request traffic data from telecommunications operators,[87] as well as communication data from securities trading companies, data provision services, credit institutions, supervised entities, and financial institutions.[88] Therefore, the vocabulary used at the national level to define entities subject to data requests by administrative authorities shows varying degrees of alignment with EU definitions.

The vocabulary issues aside, specific powers are usually granted to competition, data and financial institutions supervisors, as a transposition of

[82] Lassalle, (n. 2), p. 174.
[83] Ni Loideain, (n. 12), p. 245.
[84] Lannier, Tosza, (n. 5), pp. 301.
[85] *Ibid.* pp. 307-308.
[86] Lasagni, (n. 17), pp. 271-272.
[87] Blume et al., (n. 18), p. 207.
[88] *Ibid.* p. 229.

EU law, but these powers tend to extend the scope set for such powers under EU legislation, as they are created in other areas of enforcement.[89]

3.1.2. Categories of data under specific powers

The types of data that administrative authorities may request under their national frameworks vary significantly, reflecting differing national approaches to balancing investigatory needs with data protection and privacy safeguards. Overall, while some countries provide detailed definitions of data categories (e.g., Germany), others adopt broader or less defined terms (e.g., France and Luxembourg). In countries granting some administrative authorities with specific powers to request data from OSPs, there are discrepancies in the scope of data that may be accessed at national level among areas of enforcement. Exclusions, especially regarding sensitive data such as dynamic IP addresses, are still little considered.

In France, administrative authorities may only request, under specific powers to gather data from OSPs, one category of data, namely, 'telecommunication metadata', which may be gathered from entities subject to data retention obligations. Yet, the law does not clearly define the scope of this data category.[90]

Germany provides a detailed classification of data types. All authorities may request subscriber data—such as telephone numbers, names, addresses, dates of birth, device numbers, and contract details—, including voluntarily stored data like usernames, passwords, and PINs. However, this excludes login data related to end devices or separate storage devices.[91] The financial institutions supervisors may request traffic data, which includes call and connection details (e.g., port identifiers, card numbers, timestamps, and data volumes)[92] and communication data like call recordings and electronic messages, but access is limited to historical (past) data due to privacy protections.[93] In all cases, requests only regard stored, that is, past, data. Importantly, dynamic IP addresses are excluded due to constitutional protections of telecommunications secrecy and the 'double door model'.[94]

---

[89] Franssen, Vandormael, (n. 6), pp. 85, 87, see for instance, Article 69.2(d) of Directive 2014/65/EU of the European Parliament and of the Council of 15.05.2014 on markets in financial instruments; Article 98.1(d) of Directive 2009/65/EC of the European Parliament and of the Council of 13.07.2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities.
[90] Lassalle, (n. 2), p. 173.
[91] Blume et al., (n. 18), p. 217-218.
[92] *Ibid.* pp. 227-228.
[93] *Ibid.* p. 228.
[94] *Ibid.* p. 219.

Other countries rely on multiple or vague categories of data, allowing, in theory, to request disclosure of any kind of data. In Belgium, the competition authority may access traffic data, location data, and other electronic records from communications operators.[95] The Belgian financial markets and data protection authorities may obtain data identifying subscribers or habitual users of electronic communication services.[96] Additionally, the Belgian financial markets authority may request telecommunication calls data, such as the origin or destination of the telecommunication.[97] The data protection authority may request any data necessary to identify subscribers or regular users of devices. In Luxembourg, the financial institutions authorities may access traffic data from certain OSPs, defined as data processed for routing communications or billing purposes, and distinguished from location data.[98] Luxembourg also allows the collection by the same authorities, from anyone, of telephone recordings, electronic communications, records of data exchanges, and broader categories of 'electronic records'.[99] In Italy, the financial supervisor may access recordings of telephone conversations, electronic communications, and data exchange or any type of personal data from anyone in the context of market abuse or from supervised entities and telecommunication operations in other areas of financial law, and traffic data from providers in both cases. However, addressees may invoke secrecy to refuse to provide data.

3.1.3. Conditions to request data from certain OSPs

The conditions under which administrative authorities may request data from OSPs reveal a complex interplay of legal safeguards, investigative thresholds, and procedural requirements. While the principle of necessity emerges as a common baseline, its interpretation and application vary widely, often, intersecting with other conditions such as proportionality, relevance, and the existence of a reasonable suspicion. In some legal systems, these conditions are cumulative and tightly regulated while in others, they are loosely defined or sector-specific, leaving room for discretion and legal uncertainty. This diverse landscape reflects varying balances between investigative needs and the protection of fundamental rights across national frameworks.

The conditions under which administrative authorities may request data from certain OSPs often reflect the severity of the offence and the necessity of the data. In France, telecommunication metadata access is strictly tied to

[95] Franssen, Vandormael, (n. 6), pp. 100-101.
[96] *Ibid.* p. 102.
[97] *Ibid.* p. 96.
[98] Lannier, Tosza, (n. 5), p. 301.
[99] *Ibid.* p. 308.

the nature of the offence: customs authorities may only request such data for enumerated serious offences such as intentional smuggling and customs fraud,[100] VAT authorities for aggravated administrative offences, e.g. underreporting,[101] and the financial markets authority exclusively for market abuse investigations.[102] In Italy, data may only be requested for investigations specifically relating to market abuse.[103] Differently, the French[104] and Italian[105] competition authorities may request such data generally to investigate any anti-competitive practices. Similarly, in Germany, requests for subscriber data to digital service providers are limited to regulatory offences where fines exceed 15.000 euros, encompassing such areas as VAT violations, banking, financial markets, and GDPR breaches.[106]

One of the requirements to obtain data is the need to demonstrate the necessity of the data for the investigation in question. In Germany, requests for subscriber data must be based on an initial suspicion and must be necessary to establish facts or locate a suspect.[107] The access to traffic data by the financial institutions supervisors requires a facts-based suspicion of a breach and proof that the data is necessary for investigation.[108] In Italy, the data must as well be necessary for the investigation of market violations.[109] In Luxembourg, financial institutions authorities must show a reasonable suspicion of an infringement and that the requested records are likely to aid in establishing the truth.[110] In Ireland, any person may be asked by the VAT authority to provide reasonable assistance when exercising its powers.[111] A similar principle can be found under Polish law, as the data must be relevant for the ongoing case.[112] Additionally, in Poland, although requesting telecommunications is theoretically possible, telecommunications secrecy would require that parties to the communications should consent to its disclosure by the requested OSP.[113]The requirement of judicial authorisation or of approval by an independent body to access data varies across jurisdictions, reflecting different approaches to safeguarding privacy and ensuring proportionality. While the lack of authorisation from an independent

[100] Lassalle, (n. 2), p. 176.
[101] *Ibid.* p. 177.
[102] *Ibid.* pp. 180-181.
[103] Lasagni, (n. 17), p. 272.
[104] Lassalle, (n. 2), p. 182.
[105] Lasagni, (n. 17), p. 280.
[106] Blume et al., (n. 18), pp. 218, 227, 229, 236.
[107] *Ibid.*
[108] *Ibid.* p. 228.
[109] Lasagni, (n. 17), p. 273.
[110] Lannier, Tosza, (n. 5), p. 307.
[111] Ni Loideain, (n. 12), p. 263.
[112] Kaszubowski, Steinborn, (n. 26), p. 381.
[113] *Ibid.* p. 384.

body to request identification data could be compliant with the case law of the European Court of Justice (ECJ),[114] such situation is nevertheless questionable given the lack of clear delimitation of data categories (see *supra*, Section 3.1.1)

In France, customs authorities must obtain authorisation from the public prosecutor to access data from OSPs.[115] The authorisation of a public prosecutor is similarly required for requests to traffic data providers, telecommunication operators or other non-supervised entities by the Italian financial market supervisory authority – although a similar request under the criminal framework requires a judge authorisation.[116] Differently, in France in the context of VAT-related investigations, financial market supervision, as well as competition enforcement, requests for data must be approved by a specialised independent body: the controller of requests for telecommunication metadata.[117]

In Germany, the access to traffic data by the financial institutions supervisors requires a court order.[118] Specific requests for login data from telecommunications services also necessitate judicial authorisation.[119] In Belgium, the competition and the financial markets authorities must obtain prior authorisation from an investigating judge for data access.[120] However, the access to identification data by the financial markets and data protection authorities does not require any authorisation.[121] In Luxembourg, authorities in the financial institutions sectors must submit a reasoned request to an investigating judge.[122]

3.2. General administrative powers to gather information

Aside specific powers to request data specifically from OSPs, administrative authorities are also granted general administrative powers to gather information from third parties, namely, any persons, legal or natural, not involved in the proceedings. These general powers are typically framed in technologically neutral terms, allowing authorities to request or inspect a broad range of materials, including digital data, without necessarily invoking specialised legal regimes. However, the breadth of these powers varies

---

[114] ECJ, *La Quadrature du Net and Others v. Premier ministre and Ministère de la Culture*, 30.04.2024, C-470/21.
[115] Lassalle, (n. 2), p. 176.
[116] Lasagni, (n. 17), pp. 273.
[117] Lassalle, (n. 2), pp. 178, 180-181, 183.
[118] Blume et al., (n. 18), p. 228.
[119] *Ibid.* p. 220.
[120] Franssen, Vandormael, (n. 6), p. 91.
[121] *Ibid.* pp. 91, 96, 102.
[122] Lannier, Tosza, (n. 5), p. 307.

significantly across jurisdictions. Some countries provide overarching frameworks applicable across sectors, while others rely exclusively on sector-specific provisions. Moreover, the scope of entities subject to such requests, the types of data accessible, and the procedural safeguards in place differ widely. This section offers a comparative reflection on how these general powers are structured, highlighting the tension between administrative flexibility and the need for legal certainty, especially when such powers are used to obtain electronic evidence from actors not directly subject to supervision, such as OSPs.

3.2.1. Categories of third parties as addressees to general powers to request information

Administrative authorities across various jurisdictions generally possess broad and technologically neutral powers to request and copy information or documents,[123] either available across various sectors or sectorial, extending their scope beyond traditional paper records to include digital data. These powers typically apply to a wide range of entities, including businesses, individuals, and third parties who may hold relevant information. Additionally, search and seizure powers, traditionally used for physical records, are increasingly being leveraged to access digital data, though they often come with stricter procedural safeguards.

Only two countries rely on powers available across various sectors. In the Netherlands, the General Administrative Law Act grants all administrative authorities the right to require 'anyone' to provide information and to inspect business documents and records, which in practice has been interpreted to include data.[124] In addition to these powers available across sectors, the Netherlands provides financial market authorities with the ability to request information and to obtain business documents and records from 'anyone' when performing statutory market surveillance duties.[125] Germany also provides for investigative powers available across sectors, namely a general investigative clause provides a broad right to request any kind of information relevant to an investigation. However, compliance is not mandatory for OSPs, reflecting a potential limitation in enforcement.[126] German law also includes a general obligation for individuals to surrender objects relevant to an investigation.[127] The German Federal Constitutional Court has interpreted that the concept of "objects" in that context includes non-tangible objects, i.e.

[123] The power to copy information is notably absent from the general power of the Dutch financial market authority, De Vries et al., (n. 1), p. 355.
[124] *Ibid.* p. 339.
[125] *Ibid.* p. 355.
[126] Blume et al., (n. 18), pp. 225-226.
[127] *Ibid.* p. 223.

data.[128] In addition to these powers available across sectors, Germany also regulates sector-specific powers, such as in VAT enforcement, where authorities may request information from 'any person',[129] and German competition authorities have the power to request information from companies, associations of companies, legal entities, and associations of persons.[130]

Remaining countries rely exclusively on sectorial powers granted to administrative authorities and do not benefit from a general administrative proceedings' framework. In France, authorities in the area of banking law and financial markets as well as the data protection authority are empowered to collect information from "any person".[131] Likewise, in Belgium, competition and financial market authorities, as well as the VAT administration,[132] may request information from any natural or legal person;[133] in Luxembourg, competition, VAT and (most) financial market laws apply broadly to any person, including those holding information indirectly related to the investigated matter.[134] In Finland,[135] as well as in Italy,[136] VAT,[137] competition[138] and financial institutions authorities also have a general power to request information from third parties.[139] In Italy, the definition of customs economic operators is notably broad, extending the authorities' powers even to third parties to the investigation, which might thus encompass OSPs.[140] In Poland, the competition authority may request information from any corporation, any other natural or legal person as well as organisational units.[141]

Despite these broad general powers, different restrictions on the scope of entities subject to information requests may limit the effective use of such powers to OSPs being third parties to the investigations. For example, in France, customs authorities may only request data from individuals or entities

---

[128] *Ibid.* p. 224.
[129] *Ibid.* pp. 226-227.
[130] *Ibid.* p. 230.
[131] Lassalle, (n. 2), pp. 187, 190.
[132] Franssen, Vandormael, (n. 6), p. 89.
[133] *Ibid.* p. 90.
[134] Lannier, Tosza, (n. 5), pp. 304, 309, 317.
[135] Aside administrative authorities, under the Administrative Judicial Procedure Act, the Market Court has the authority to compel the production of documents and objects as evidence in competition cases, extending this obligation to a wide range of third parties, Riekkinen, (n. 3), p. 135.
[136] Lasagni, (n. 17), pp. 275, 280.
[137] Riekkinen, (n. 3), p. 140.
[138] *Ibid.* p. 148.
[139] *Ibid.* p. 145.
[140] Lasagni, (n. 17), p. 278.
[141] Kaszubowski, Steinborn, (n. 26), p. 382.

'directly or indirectly involved' in customs-related operations.[142] Similarly, in the Netherlands, tax authorities may request information only from third parties legally required to maintain tax records, while customs authorities limit their requests to those involved in customs formalities or controls.[143] Finland[144] and Luxembourg[145] follow similar approaches, limiting customs-related requests to entities holding information necessary for customs taxation or operations. Other powers are restricted to supervised entities or related ones, which might thus exclude OSPs. In Finland, certain powers of the financial institutions supervisors are specifically designed to target supervised entities and other financial market participants, limiting the scope of information requests to those directly involved in regulated activities.[146] Similarly, in Luxembourg, some financial markets and banking laws restrict information requests to supervised entities, but they may also extend to persons with a direct link to supervised activities, such as auditors or other professionals involved in financial operations.[147]

In the context of data protection enforcement, the scope of investigative powers granted under the GDPR has been extended at the national level to varying degrees across jurisdictions. While the GDPR primarily empowers authorities to request information from controllers or processors—usually understood as the investigated entity—some countries have broadened these powers to include third parties. In the Netherlands, the data protection authority may request information from 'anyone', extending their reach beyond the direct subjects of investigation.[148] Similarly, in Finland, the data protection authority may also obtain information from any third parties.[149] Such an extension is also contemplated in the investigation of internal rules of the Luxembourg data protection authority, although not provided for by law, raising a legality issue.[150] In Belgium, the data protection authority extends its reach to require the identification of the subscribers or habitual users of an electronic communication service.[151] In contrast, Germany takes a more restrictive approach, interpreting the GDPR as conferring only general supervisory and inspection powers, without extending to administrative

[142] Lassalle, (n. 2), p. 185.
[143] De Vries et al., (n. 1), p. 353.
[144] Riekkinen, (n. 3), p. 138.
[145] Lannier, Tosza, (n. 5), p. 302.
[146] Riekkinen, (n. 3), p. 145.
[147] Lannier, Tosza, (n. 5), pp. 309-310.
[148] De Vries et al., (n. 1), p. 362.
[149] Riekkinen, (n. 3), p. 154.
[150] Lannier, Tosza, (n. 5), p. 321.
[151] Franssen, Vandormael, (n. 6), pp. 101-102.

punitive proceedings that could compel third parties to provide information.[152]

Powers for search and seizure, traditionally used to physically obtain documents and records, can also be leveraged to request information from third parties in certain jurisdictions. For instance, in France, VAT authorities may seize 'documents and records' including in the form of data, under the condition of judicial authorisation. However, such powers can only be exercised if there are indications of fraud, such as issuing fictitious invoices.[153] Similarly, competition authorities may seize business records stored on any medium within business premises.[154] The French data protection authority may also access any location where personal data is processed, contingent on judicial approval.[155] Similarly, the Belgian data protection authority may perform on-site examination and consult, copy or seize computer systems containing personal data.[156] In Finland, competition authorities conducting on-site inspections have the right to obtain all necessary information, including from service providers managing communications or data on behalf of the investigated entity.[157] Belgium takes a more detailed approach, particularly regarding IT seizures during competition inspections, requiring judicial authorisation and legal representation among other requirements.[158] These physical document requests, which have not fully adapted to the digital nature of modern investigations, provide stronger procedural safeguards akin to those in criminal investigations, compared to general powers to request information.

As a general rule, administrative authorities across all examined jurisdictions must adhere to the principle of territoriality when exercising their investigative powers, meaning they may only request data from entities operating within their national borders. However, under German law, authorities may request data not only from entities physically established in Germany but also from any private actor providing services within the country, regardless of their physical presence. This criterion extends investigative powers beyond territorial boundaries by targeting service providers that offer services to users in Germany or merely maintain a branch in the country. Such an approach effectively broadens the scope of German authorities' data access capabilities, allowing them to reach foreign-based companies with operations or commercial interests in Germany, thereby

[152] Blume et al., (n. 18), p. 234.
[153] Lassalle, (n. 2), pp. 186-187.
[154] *Ibid.* pp. 187-190.
[155] *Ibid.* p. 190.
[156] Franssen, Vandormael, (n. 6), pp. 101-102.
[157] Riekkinen, (n. 3), p. 150.
[158] Franssen, Vandormael, (n. 6), p. 101-102.

circumventing strict territorial limitations typically applied in other jurisdictions.[159]

3.2.2. Conditions to request information to third parties

The conditions for implementing general powers to request data appear to be generally less stringent than those governing specific powers. While the principle of necessity is a common denominator, its interpretation ranges from a minimal threshold of relevance to more demanding standards requiring justifiable cause or specificity. In France, for example, customs authorities may request information deemed 'of interest',[160] while under the Monetary and Financial Code, data may be obtained 'for the purposes of the investigation', suggesting a relatively low threshold for data requests.[161] Similarly, in Luxembourg, customs authorities may seek 'any information deemed necessary',[162] whereas VAT authorities may request data whenever it is necessary to detect tax infringements and ensure proper tax collection.[163]

Both the Luxembourg[164] and Belgian[165] competition authorities may gather 'necessary' information. Finnish financial institutions authorities may obtain data from individuals who can be 'presumed with justifiable cause' to hold 'necessary' information,[166]; and data protection authorities may request information that is necessary for fulfilling their tasks.[167] Luxembourg's financial institutions authorities operate under a broader framework, allowing them to request information that may be considered likely to be relevant for their supervisory, investigatory, or other functions,[168] which underlines the lack of clear separation between supervisory and investigatory competences.

Similarly, the German competition authorities may use their powers either for general supervision or targeted investigations, with the latter requiring an initial suspicion. Deadlines for compliance are usually left to the discretion of the requesting authority, though German case law has deemed periods between two to four weeks to be reasonable.[169] In Luxembourg, VAT compliance deadlines in practice range from one week to over a month.[170] Italy is an exception in that the competition authorities may request all the

[159] Blume et al., (n. 18), p. 224.
[160] Lassalle, (n. 2), p. 185.
[161] *Ibid.* p. 187.
[162] Lannier, Tosza, (n. 5), p. 302.
[163] *Ibid.* p. 303.
[164] *Ibid.* p. 317.
[165] Franssen, Vandormael, (n. 6), p. 89.
[166] Riekkinen, (n. 3), p. 145.
[167] *Ibid.* p. 154.
[168] Lannier, Tosza, (n. 5), p. 311.
[169] Blume et al., (n. 18), p. 233.
[170] Lannier, Tosza, (n. 5), p. 303.

information deemed necessary, however, the deadline for compliance shall not exceed sixty days. This time limit may be extended upon a reasoned request.[171] Furthermore, Italian customs authorities have the power to request information, to be provided within at least fifteen days.[172]

In Poland, competition authority mostly relies on search and seizures to obtain data and enter IT systems. However, because of the principle of proportionality the exercise of this power against third party is merely subsidiary: it may only be conducted against them if the same action is not possible against the investigated person.[173]

Some jurisdictions impose stricter procedural requirements in some areas of enforcement, particularly formalities related to the content of requests can also vary. In Luxembourg, competition authorities must first open a formal procedure before issuing an information request, and the request must explicitly state the object and purpose, failing which it may be declared null and void.[174] Requests by the German competition authorities must specify the legal basis, the object and purpose of the request, and a reasonable deadline.[175] Similarly, Italian competition authorities, must specify the legal grounds for the request.[176] In Finland, VAT-related data requests must identify the taxpayer by name, bank account number, or another specific identifier, preventing fishing expeditions but allowing for requests without personal identification if other specific details are provided;[177] and in Finland's financial institutions sector, data requests are usually issued in writing, specifying the information sought and the legal basis for the request.[178] In Germany, VAT data requests follow a layered approach, targeting any person and subsidiarily the taxpayer for taxation purposes.[179]

3.2.3. Categories of data under general powers

The general powers, as previously defined, are not confined to specific sectors or to specific categories of actors, and are typically framed in broad, technologically neutral terms. As a result, they often allow authorities to request a wide range of data, from traditional business records to digital content such as emails, metadata, or system logs. However, the breadth and precision of these powers vary significantly across jurisdictions. Some legal

[171] Lasagni, (n. 17), p. 276.
[172] *Ibid.* p. 279.
[173] Kaszubowski, Steinborn, (n. 26), p. 384.
[174] Lannier, Tosza, (n. 5), p. 318.
[175] Blume et al., (n. 18), p. 232.
[176] Lasagni, (n. 17), p. 276.
[177] Riekkinen, (n. 3), p. 141.
[178] *Ibid.* p. 146.
[179] Blume et al., (n. 18), pp. 226-227.

systems explicitly include digital formats and define the scope of accessible data in detail, while others rely on vague or outdated terminology, leaving room for interpretation. Moreover, the extent to which sensitive or privileged data can be accessed under general powers is unevenly regulated.

The breadth of categories of data that can be requested under general powers is extensive across various jurisdictions, encompassing both paper and digital formats. In the Netherlands, authorities may request a wide array of 'records', which includes data such as GPS registrations, email data, mailboxes, USBs, and even more specific items such as draft accounts, till rolls, microfilms, and order confirmations.[180] The Dutch data protection authority may explicitly request telemetry data, which covers information about the transmission of personal data to other devices.[181] In Luxembourg, customs authorities may obtain documents and correspondence,[182] while the VAT authority, like in Ireland,[183] may demand all information related to taxable operations.[184] The French data protection authority may request all types of documents and even computer programs.[185] Finnish competition and data protection authorities are likewise empowered to request all types of data.[186] Also Italian authorities may obtain copies of all types of documents, including access to databases.[187]

The breadth of the scope is particularly extensive for competition and financial institutions authorities. In Germany, competition authorities may demand all original documents in any form, including data storage locations and passwords,[188] as long as the data is accessible within the economic unit.[189] Belgium grants competition authorities the power to access digital evidence, such as electronic and instant messages, irrespective of their storage location, whether on local servers or in the cloud.[190] The Dutch competition authority further clarifies that its data requests may include content and metadata as long as related to business information, such as emails, chat applications, and document edits.[191] In Luxembourg, the financial institutions authorities,[192] as well as the competition authority, may access any document, information, or

[180] De Vries et al., (n. 1), pp. 340, 353.
[181] *Ibid.* p. 363.
[182] Lannier, Tosza, (n. 5), p. 302.
[183] Ni Loideain, (n. 12), p. 262.
[184] Lannier, Tosza, (n. 5), p. 303.
[185] Lassalle, (n. 2), p. 190.
[186] Riekkinen, (n. 3), pp. 148, 154.
[187] Lasagni, (n. 17), p. 284.
[188] Blume et al., (n. 18), p. 230.
[189] *Ibid.* p. 232.
[190] Franssen, Vandormael, (n. 6), p. 99.
[191] De Vries et al., (n. 1), pp. 357-358.
[192] Lannier, Tosza, (n. 5), p. 310.

data available to the addressee, including software data for the latter.[193] Finland explicitly includes recordings of telephone conversations, electronic communications, telecommunications data, and information systems within the scope of data requests by the financial institutions authorities.[194] The Italian competition authority may access all electronic communications, including recordings,[195] the customs authority may access all data and documents related to taxes in the broad sense,[196] while the VAT authority may demand documents and invoices relating to transactions.[197]

However, such broad scopes are restricted in some jurisdictions based on a balancing exercise with the protection of fundamental rights. Some of these restrictions derive from the same legislations on administrative proceedings. In France, customs and financial market authorities have broad powers to access 'papers and documents, whatever the medium', implying an all-encompassing scope that includes data.[198] However, the scope must exclude telecommunication metadata, which request is specifically regulated under a different power (see Section 2.1). In Finland, traffic and content data related to electronic communications may only be acquired from supervised entities, limiting the scope of data requests in the financial institutions sector.[199]

Furthermore, all jurisdictions restrict the scope of the gathering of information through the protection of different professional secrecy. In the Netherlands, authorities cannot request personal or non-business documents, and business documents covered by legal professional privilege are also protected. Dutch law recognises the secrecy of information received by lawyers,[200] as well as similar protections for clergymen, notaries, doctors, and pharmacists in tax matters.[201] Similarly, Germany imposes stricter frameworks and guarantees for data that require heightened protection, such as due to the legal professional privilege.[202] Conversely, Luxembourg's financial institutions laws prevent the use of professional secrecy to refuse cooperation, except in market abuse cases.[203] In Finland, certain individuals have a general right not to testify, such as due to a professional secrecy;

[193] *Ibid.* p. 317.
[194] Riekkinen, (n. 3), p. 145.
[195] Lasagni, (n. 17), p. 275.
[196] *Ibid.* pp. 278-279.
[197] *Ibid.* p. 280.
[198] Lassalle, (n. 2), pp. 185-187.
[199] Riekkinen, (n. 3), p. 146.
[200] De Vries et al., (n. 1), p. 341.
[201] *Ibid.* pp. 345-346.
[202] Blume et al., (n. 18), p. 224.
[203] Lannier, Tosza, (n. 5), p. 312.

however, this does not extend to disclosing information about their financial situation in customs and VAT matters.[204]

However, there is no standardised regulatory framework for filtering privileged data in any of the studied jurisdiction, except in the Netherlands. The Dutch financial market authorities have implemented a binding regulation detailing a multi-step process to clean data, involving IT specialists, notification to the investigated party, and possible remedies before civil courts.[205] A different approach is followed by the Dutch competition and data protection authorities, which establish a 'within-the-scope' dataset before allowing an overview to the concerned person, who can then request filtering of potentially irrelevant information, subject to review by a legal professional privilege officer.[206] In France, the data protection authority is restricted from accessing data protected by legal professional secrecy, journalistic secrecy, and medical secrecy.[207]

In addition to sector-specific and procedural restrictions, the scope of administrative authorities' investigative powers is also limited by constitutional and European frameworks that limit data collection. In the Netherlands, the Supreme Court has ruled that intrusive investigative techniques, such as placing GPS trackers on vehicles or accessing automatic license plate recognition systems used by the police, are not permissible for administrative enforcement purposes, as they constitute a serious interference with private life under European Court of Human Rights (ECtHR) case law.[208] Furthermore, Dutch authorities face restrictions in accessing traffic and location data, which is primarily reserved for criminal proceedings and requires prior judicial authorisation.[209]

Similarly, in Finland, the Constitution allows for limitations on the secrecy of communications for criminal investigations but does not extend the same permissions to punitive administrative proceedings. Finnish constitutional doctrine establishes that administrative investigations cannot, in practice, employ covert measures equivalent to telecommunications interception or traffic data monitoring.[210] Luxembourg and Germany impose notable constitutional and statutory limits on administrative access to electronic communication data, reserving it for criminal proceedings and excluding professional data from constitutional coverage.[211] Germany applies

[204] Riekkinen, (n. 3), pp. 138, 140.
[205] De Vries et al., (n. 1), pp. 355-357.
[206] *Ibid.* pp. 360-362.
[207] Lassalle, (n. 2), p. 191.
[208] De Vries et al., (n. 1), p. 343.
[209] *Ibid.* p. 344.
[210] Riekkinen, (n. 3), p. 146.
[211] Lannier, Tosza, (n. 5), pp. 324-325.

a ‘double-door model’, requiring both a legal basis for the authority’s request and a separate one for the OSP’s disclosure.[212]

3.3. Transfer of data and enforcement of orders

This section explores how administrative authorities across jurisdictions operationalise their powers to gather electronic evidence, focusing on two key dimensions: the transfer of data and the enforcement of requests when OSPs do not conform to these. The comparative analysis reveals that while some jurisdictions have developed secure and formalised systems for data transmission, others rely on informal or inconsistent practices. Similarly, enforcement mechanisms vary widely: some legal systems provide strong coercive tools such as fines, administrative penalties, or even criminal sanctions, while others offer limited or no means to compel third-party cooperation, which is similar to criminal law.[213] These disparities affect not only the efficiency of administrative investigations but also the legal certainty and accountability of data collection practices.

3.3.1. Data transfer

The transfer of data requested by administrative authorities under both general and specific powers is subject to relatively few formal conditions and rules across jurisdictions. the transfer of data, once requested by administrative authorities, is diversely regulated and implemented in practice across jurisdictions. Indeed, the analysis reveals a fragmented landscape: while some countries have implemented secure and formalised channels, such as encrypted platforms or structured formats, others rely on *ad hoc* methods like email or postal delivery, often lacking consistency and reliability. Requirements concerning the readability, confidentiality, and integrity of transferred data also vary, with only a few jurisdictions imposing clear obligations on format or ensuring that sensitive data is adequately protected during transmission. Moreover, rules on data retention and destruction are often sector-specific and inconsistently applied, raising concerns about proportionality and long-term data protection. These divergences highlight the operational challenges of digital evidence gathering and underscore the need for clearer, harmonised standards to ensure both the effectiveness and the accountability of administrative data transfers.

In Germany, subscriber data must be transferred ‘without delay and at the requesting party’s expense’, with a requirement to maintain confidentiality regarding the request. Additionally, telecommunications

[212] Blume et al., (n. 18), pp. 212-213.
[213] Franssen, Tosza, (n. 76).

service providers with more than 100,000 customers must ensure a secure electronic interface for data transfer, which can take the form of an email-based procedure or a dedicated electronic platform.[214] For competition matters, data must be provided electronically via an online platform.[215] In Finland, customs, data protection and VAT-related data requests must also be transferred at the entity's expense.[216] In France, the VAT authority mandates data transmission through a secure system.[217] In Luxembourg, VAT-related data may be exchanged through a dedicated platform provided by the administrative authority when large data volumes are involved. However, in practice, the platform seems to be oftentimes unreliable, resulting in data being transferred via email, post, or a combination of both.[218]

Regarding the format of transferred data, several jurisdictions impose requirements to ensure accessibility of computer programs and data. In France, the data protection authority mandates that such information should be transcribed into a format that is intelligible.[219] Similarly, Luxembourg's customs and VAT laws require data to be provided in a readable and comprehensible form.[220] Luxembourg competition authority may request that data be transcribed into documents.[221] The Luxembourg competition authority further specifies that data must be provided in a clear way, meaning it should not be encrypted.[222] The Netherlands also incorporates encryption measures in competition investigations, by applying a hash to ensure the integrity and security of the dataset throughout the process.[223]

Examined legal orders provide also rules as regards protection of data collected by administrative authorities as well its mandatory destruction. In France, the VAT law requires storage measures that guarantee confidentiality.[224] Similarly, the financial markets authority imposes strict storage protocols to preserve confidentiality,[225] while the competition authority ensures that data is both transmitted and stored securely.[226] In Germany, telecommunications service providers must provide a secure electronic interface that safeguards data integrity and maintains logs to track

---

[214] Blume et al., (n. 18), pp. 220-221.
[215] *Ibid.* p. 230.
[216] Riekkinen, (n. 3), pp. 139, 141, 154.
[217] Lassalle, (n. 2), p. 178.
[218] Lannier, Tosza, (n. 5), p. 303.
[219] Lassalle, (n. 2), p. 190.
[220] Lannier, Tosza, (n. 5), pp. 302, 303.
[221] *Ibid.* p. 317.
[222] *Ibid.*
[223] De Vries et al., (n. 1), p. 360.
[224] Lassalle, (n. 2), p. 178.
[225] *Ibid.* p. 182.
[226] *Ibid.* p. 184.

access.[227] In Finland, in cases involving large datasets, practical aspects such as data security and pseudonymisation are typically discussed in advance between the competition authority and the responding party to address potential challenges before an official request is made.[228]

With regard to data destruction, few jurisdictions have set time limits for how long data can be stored, and those rules are usually provided on sectoral level. In France, customs data must be deleted once tax penalties are enforced,[229] while VAT-related data must be retained for one year or until the conclusion of all appeal procedures.[230] The financial markets authority requires data to be destroyed one month after the Board's decision or six months after the final ruling of the Enforcement Committee or appeal courts if a notification of grievance has been issued; however, data transferred to criminal proceedings may be retained for longer.[231] The competition authority follows a similar approach, with data deleted six months after a final decision or within one month if the information pertains to facts that are not prosecuted.[232] In the Netherlands, the financial markets authority's working methods specify that raw data should be deleted once a clean dataset has been produced , or if it is determined that certain data should have been excluded from the investigation.[233]

3.3.2. Enforcement of requests

While administrative authorities across jurisdictions are increasingly empowered to request data from third parties, the effectiveness of these powers ultimately depends on the availability and strength of enforcement mechanisms to ensure compliance: mechanisms that vary widely in scope, intensity, and applicability. The enforcement of administrative authorities' data requests is typically executed by means of general statutory obligations to cooperate, applying both to specific and general powers. Coercive fines or penalty payments are used to ensure compliance under some legal frameworks.

The enforcement of data requests through coercive fines varies widely across jurisdictions in both scope and severity. Some countries, such as Germany[234] and Luxembourg,[235] impose substantial financial penalties—

[227] Blume et al., (n. 18), p. 221.
[228] Riekkinen, (n. 3), p. 150.
[229] Lassalle, (n. 2), p. 176.
[230] *Ibid.* p. 178.
[231] *Ibid.* p. 181.
[232] *Ibid.* p. 184.
[233] De Vries et al., (n. 1), pp. 356-357.
[234] Blume et al., (n. 18), p. 234.
[235] Lannier, Tosza, (n. 5), p. 318.

often calculated as a percentage of a company's global turnover—for non-compliance, particularly in competition law. Ireland[236] and Italy[237] provide for high maximum coercive fines in the financial and competition sectors. France[238] and Luxembourg[239] also apply daily fines, though in Luxembourg these are often limited to supervised entities, excluding third parties like OSPs.[240] In contrast, Finland adopts a more cautious model: fines require judicial approval or are only imposed in cases of non-negligent non-compliance.[241] Meanwhile, the Netherlands stands out for lacking coercive fines altogether in this context.[242]

In some jurisdictions, failure to comply with data requests does not result in any sanctions, particularly for third parties, effectively relying on voluntary cooperation. For instance, in Poland, no specific enforcement measure exists.[243] In Italy, no enforcement mechanisms is provided for specific request of data by the financial supervisor.[244] In the Netherlands, under competition and data protection laws, only the investigated party may be sanctioned, not third parties.[245] Similarly, Finnish competition authority may impose fines for providing false, insufficient, or misleading information, but these are typically limited to undertakings under investigation, making their applicability to third parties unlikely according to the literature.[246] Raising the same question, the Luxembourg competition authority, as well as the Italian competition authority,[247] may impose fines to undertakings, understood as those under investigation and not third parties, if failing to comply with a request for information.[248]

Administrative fines for non-compliance with data requests vary widely in amount, scope, and legal basis across jurisdictions. The general tendency shows low fines under customs frameworks, compared to highest ones available to competition and financial regulators. France and Luxembourg impose sector-specific fines ranging from modest daily penalties (e.g., €150 in French customs or €250–10,000 in Luxembourg VAT)[249] to substantial

---

[236] Ni Loideain, (n. 12), p. 255.
[237] Lasagni, (n. 17), p. 276.
[238] Lassalle, (n. 2), p. 176.
[239] Lannier, Tosza, (n. 5), p. 304.
[240] *Ibid.* p. 312.
[241] Riekkinen, (n. 3), p. 146, 151.
[242] De Vries et al., (n. 1), p. 342.
[243] Kaszubowski, Steinborn, (n. 26), pp. 384-385.
[244] Lasagni, (n. 17), p. 274.
[245] De Vries et al., (n. 1), pp. 359, 364.
[246] Riekkinen, (n. 3), p. 152.
[247] Lasagni, (n. 17), p. 274.
[248] Lannier, Tosza, (n. 5), p. 318.
[249] *Ibid.* p. 304.

amounts in financial sectors—up to €5 million or 10% of annual turnover.[250] Germany combines low general fines with higher competition-related penalties,[251] while Italy's VAT and financial regulators may impose fines up to €8,000 and €5 million respectively.[252] In Finland, fines are more moderate and often tied to negligence, with a €15,000 cap in VAT enforcement.[253]

In some jurisdictions, failure to comply with administrative data requests may trigger criminal liability, though the scope and severity of sanctions vary considerably. The Netherlands criminalises general non-cooperation, including by third parties and OSPs, with penalties up to three months' imprisonment.[254] France[255] and Luxembourg impose criminal penalties across multiple sectors, with fines reaching up to €125,000 and prison sentences of up to five years, particularly in financial and securities regulation.[256] Italy applies criminal sanctions more selectively—typically for providing false information or obstructing investigations—with VAT-related violations carrying prison terms of up to seven years.[257]

4. LEGAL SAFEGUARDS IN ADMINISTRATIVE INVESTIGATION PROCEEDINGS

Legal safeguards in administrative investigation proceedings are unevenly developed across jurisdictions, particularly when it comes to protecting third parties such as OSPs. While most legal systems formally recognise core principles, like the right to be heard, protection against self-incrimination, and access to remedies, their practical application is often limited or unclear. Safeguards tend to focus on the investigated person, leaving third parties with limited procedural rights and unclear guidance on how to challenge data requests. Judicial oversight is rarely available at the request stage, and remedies typically become accessible only once enforcement measures are imposed. Moreover, the legal status of data requests, whether they constitute appealable acts or mere preparatory steps, varies significantly, affecting the availability of procedural protections. Overall, the analysis reveals a structural gap between the expanding powers of administrative authorities to gather electronic evidence and the underdeveloped framework of safeguards designed to ensure fairness, transparency, and accountability in such proceedings.

---

[250] *Ibid.* pp. 313-314.
[251] Blume et al., (n. 18), pp. 221-222, 234.
[252] Lasagni, (n. 17), pp. 281-283.
[253] Riekkinen, (n. 3), p. 143.
[254] De Vries et al., (n. 1), p. 342.
[255] Lassalle, (n. 2), p. 184.
[256] Lannier, Tosza, (n. 5), p. 314.
[257] Lasagni, (n. 17), pp. 279, 281.

4.1. Safeguards available to third parties

Safeguards available to third parties against data requests by administrative authorities are quite limited under all studied jurisdictions and remain diverse among areas of enforcement and between specific and general powers. Some safeguards indirectly extend to third parties, including OSPs, even though they are not the primary focus of the legal frameworks. For instance, certain provisions aim to uphold the principle of non-self-incrimination when data requests risk revealing unrelated violations, while others require notification, often through record-keeping, and offer a limited right to be heard. Remedies are generally designed for the investigated person, but in some jurisdictions, they are formulated broadly enough to be invoked by third parties, including OSPs, when they are asked to produce data. However, the applicability of these safeguards to third parties remains legally ambiguous and inconsistently recognised, reflecting a broader structural gap in procedural protections for actors who are not the direct subject of investigation but are nonetheless instrumental in the evidence-gathering process.

4.1.1. Protection against self-incrimination

Examined legal orders included protection against self-incrimination of the requested third parties into proceedings in which administrative authorities gather data from third parties. This safeguard derives from the ECtHR *Saunders* case law, incorporated into national administrative punitive proceedings.[258]

For instance, in the Netherlands, if an investigation into a particular entity reveals potential violations by third parties, the authority refrains from expanding the ongoing investigation to include them. Instead, it initiates a separate enforcement procedure to ensure that third parties do not inadvertently become subjects of investigation without proper procedural safeguards.[259] Yet, third parties in the Netherlands are not protected by the privilege against self-incrimination unless the requested information directly implicates them in wrongful conduct.[260] This privilege is mostly recognised in favour of the investigated person, but it is limited to will-dependent acts. However, the privilege does not extend to documentary evidence, such as passwords or biometric data, which are considered will-independent and can be requested without violating the privilege. For instance, in competition

[258] ECtHR, *Saunders v. the United Kingdom*, 17.12.1996, no. 19187/91; S. Lamberigts, *Corporations and the privilege against self-incrimination*, Hart Publishing, Hart Studies in European Criminal Law, 2022.
[259] De Vries et al., (n. 1), p. 364.
[260] *Ibid.* pp. 346-347.

investigations, authorities are required to inform employees of the natural person under investigation of their rights, ensuring they have an opportunity to invoke the privilege.[261] Conversely, in Poland, the law explicitly allows to use data disclosed against the person at the origin of the disclosure, although the provision only refers to natural persons.[262]

Similarly, in France, the financial markets authority is explicitly authorised to implement its specific power to request data solely for the purposes of the investigation for which it has received prior authorisation, preventing any unauthorised expansion of the inquiry's scope.[263] In Finland, coercive fines are excluded in customs matters when their imposition could jeopardise the privilege against self-incrimination, while in sectors such as banking, financial markets, competition, and data protection, this safeguard applies only to natural persons.[264] In Luxembourg, the sanctioning of supervised entities in the financial institutions sector for failing to provide potentially self-incriminating information has faced criticism from legal scholars and the State Council, reflecting concerns over the balance between regulatory compliance and fundamental rights.[265] Additionally, in Luxembourg[266] and Italy's[267] competition law frameworks, requests for data must not compel undertakings to admit the existence of an infringement.

4.1.2. Notification and right to be heard

The right to be notified and to be heard are foundational principles of fair administrative proceedings, yet their application in the context of data requests to OSPs remain inconsistent and often underdeveloped. While some jurisdictions formally recognise these rights and provide mechanisms for their implementation, such as prior communication of the grounds for a decision or the opportunity to submit observations, others treat data requests as mere investigatory acts, not triggering procedural safeguards. Even where safeguards exist, they are often designed with the investigated person in mind, leaving third parties with limited or unclear entitlements.

Other safeguards relate to the recording and notification of data requests when administrative authorities obtain data from third parties. For example, in France, customs authorities are required to maintain records when exercising their specific power to obtain data from OSPs.[268] Similarly, in

[261] *Ibid.* p. 359.
[262] Kaszubowski, Steinborn, (n. 26), p. 388.
[263] Lassalle, (n. 2), p. 181.
[264] Riekkinen, (n. 3), pp. 139, 146, 151, 156.
[265] Lannier, Tosza, (n. 5), p. 313.
[266] *Ibid.* p. 318.
[267] Lasagni, (n. 17), p. 276.
[268] Lassalle, (n. 2), p. 176.

Luxembourg, customs authorities operating under their general powers must provide the owner of the record with a detailed list of the materials collected.[269]

Similarly, the right to be heard, while being an essential procedural safeguard in administrative sanctioning proceedings is often recognised as a general principle of administrative procedure especially when the sanction is qualified as criminal,[270] for instance in Poland.[271] In Finland[272] and in Belgium,[273] the Market Court, which is a judicial and not an administrative authority, ensures this right by allowing parties to present their views before issuing a production order. In Luxembourg, the framework for non-contentious administrative procedures mandates authorities to communicate the factual and legal grounds of their decisions, granting individuals eight days to submit their observations. Luxembourgish case law further emphasises that the right must be specifically detailed, rather than merely mentioned, particularly in financial sector investigations. However, failure to comply with this requirement only results in the annulment of a decision if it can be demonstrated that proper consideration would have led to a different outcome.[274] In the context of customs enforcement, Luxembourg authorities must provide prior communication of the grounds for unfavourable decisions, such as imposing an administrative fine for failure to comply with an information request, and allow a 30-day period for observations.[275] In competition law, Luxembourg authorities ensure that undertakings are notified of the objections raised against them and are given at least one month to submit their observations before the imposition of coercive or administrative fines.[276]

4.1.3. Remedies

The availability of remedies for third parties subject to data requests by administrative authorities presents significant challenges, primarily due to the uncertain legal status of such requests. In contrast, in certain jurisdictions and areas of enforcement, there are no specific remedies available to third parties. For instance, in France, the law does not provide for any remedies for third

[269] Lannier, Tosza, (n. 5), p. 302.
[270] European Court of Human Rights, *Guide on Article 6 of the European Convention on Human Rights Right to a fair trial (criminal limb)*, Council of Europe, 31.08.2022; Committee of Ministers, *Resolution (77) 31 on protection of the individual in relation to the acts of administrative authorities*, Council of Europe, 28.09.1977.
[271] Kaszubowski, Steinborn, (n. 26), p. 384.
[272] Riekkinen, (n. 3), p. 136.
[273] Franssen, Vandormael, (n. 6), p. 100.
[274] Lannier, Tosza, (n. 5), p. 298.
[275] *Ibid.* p. 303.
[276] *Ibid.* p. 319.

parties against requests for data made under both specific and general powers by authorities such as customs,[277] VAT administration,[278] and the financial markets authority.[279]

A key issue is whether these requests constitute administrative acts that may be challenged directly or if they are merely preparatory measures that do not provide an immediate right of appeal. In the Netherlands, the distinction is made between administrative decisions—defined as written decisions by an administrative body with legal effects—and factual acts. The latter may only be challenged if they contribute to the motivation of a final decision.[280] As a last resort, civil courts provide a safety net through tort actions, offering stringent judicial review to scrutinise the actions of public authorities under public law principles.[281] Similarly, in Luxembourg, competition law case law treats requests for information as mere investigatory steps rather than final administrative decisions, thereby denying third parties immediate remedies,[282] a limitation justified by courts by the need for enforcement efficiency.[283] In Finland, the situation is comparable, with requests for evidence generally not considered appealable decisions.[284] For instance, in VAT enforcement,[285] an initial written request does not carry the legal weight of an administrative decision, and in the financial institutions sector, ignoring such requests does not entail direct consequences.[286] This approach extends to competition and data protection enforcement, where only enforcement actions such as coercive fines trigger appeal rights.[287] The main advantage of this approach for authorities is that such requests are typically prepared and sent by the same investigator, often without any judicial or administrative oversight until enforcement becomes necessary.

To the contrary, remedies are available against requests if they require authorisation. Germany excludes preparatory investigative measures from appeal, but only if they lack legal significance and do not interfere with an individual's legal sphere.[288] However, judicial orders authorising investigatory measures during administrative proceedings may be subject to judicial review. If an order is issued by an administrative authority court

[277] Lassalle, (n. 2), pp. 176, 186.
[278] *Ibid.* p. 180.
[279] *Ibid.* p. 182.
[280] De Vries et al., (n. 1), p. 349.
[281] *Ibid.* pp. 351-352.
[282] Lannier, Tosza, (n. 5), p. 297.
[283] *Ibid.* p. 320.
[284] Riekkinen, (n. 3), p. 137.
[285] *Ibid.* p. 140.
[286] *Ibid.* p. 146.
[287] *Ibid.* pp. 149, 155.
[288] Blume et al., (n. 18), p. 215.

review is available only if explicitly provided by law. There remains theoretical uncertainty regarding whether a third party may make use of such a remedy based on a legitimate interest, such as the disclosure of personal data.[289] A similarly unclear situation can be found in Luxembourg as regards the third persons as the remedies seem to exclude them.[290] In France, judicial review is available if an order is issued by a judicial authority, e.g. in customs matters.[291] Naturally, remedies remain available against administrative decisions, particularly in case of enforcement of data requests, such as through coercive fines. Remedies are available against Dutch administrative decisions through internal administrative review, followed by an indirect appeal to an administrative court.[292] In Belgium, decisions made by administrative authorities in competition, financial institutions, and data protection matters—such as administrative fines—can be appealed before the Market Court, which provides judicial oversight.[293] Similarly, in Germany, third parties may seek judicial review against administrative fines, which are considered administrative acts.[294] In Finland, remedies generally consist of an administrative review followed by judicial review.[295] Some areas, such as VAT enforcement, require a mandatory administrative review by the Adjustment Board before the matter may proceed to judicial review.[296] In Luxembourg, there are multiple layers of administrative recourse against sanctions, including requesting a reassessment by the issuing authority, escalating to a hierarchical superior (e.g., a director), or appealing to the supervising authority (e.g., a ministry). Judicial review is available against any of these administrative decisions, provided that the third party can demonstrate a 'personal, direct, and legitimate interest'.[297] However, in the financial institutions sector, some legal frameworks only provide for a review of the substance of the case rather than the merits, limiting the scope of challenges.[298]

4.2. Safeguards available to the investigated person

Safeguards available to the investigated person in administrative proceedings often stem from fundamental rights principles, yet they are not always explicitly enshrined in the relevant legal frameworks. This lack of

[289] *Ibid.* pp. 214-215, 222.
[290] Lannier, Tosza, (n. 5), p. 307.
[291] Lassalle, (n. 2), pp. 178, 180-181, 183.
[292] De Vries et al., (n. 1), p. 348.
[293] Franssen, Vandormael, (n. 6), p. 99.
[294] Blume et al., (n. 18), p. 208.
[295] Riekkinen, (n. 3), p. 137.
[296] *Ibid.* p. 144.
[297] Lannier, Tosza, (n. 5), p. 300.
[298] *Ibid.* p. 316.

explicit recognition and detailed regulation raises concerns regarding legal certainty and predictability for individuals facing investigation. While some safeguards overlap with those afforded to third parties (see Section 3.1), the investigated person benefits from additional protections due to their direct involvement in the proceedings. These additional safeguards, however, remain inconsistently applied across jurisdictions and enforcement areas, leading to potential disparities in protection.

The right to notification and access to records in favour of investigated persons also varies across jurisdictions. In France, under customs law, records obtained through specific investigatory powers are systematically added to the case file.[299] In Germany, the investigated person must be notified of court decisions that affect their rights, such as requests for login data. However, there is no obligation to notify them of investigative actions taken by the public prosecution, police, or administrative authority.[300] When subscriber data is requested, notification is only required once it no longer risks compromising the investigation's purpose.[301] In the absence of notification, the fair trial principle is ensured through access to the file.[302] Furthermore, in cases of voluntary surrender or seizure of data, both the data holder (e.g., OSP) and the affected individual must be notified.[303] Luxembourg's framework on non-contentious administrative procedures grants individuals the right to access their administrative files, with exceptions for public or private interests.[304] However, in practice, access to records is often denied or not provided in VAT matters.[305] In competition law, the principle of access is upheld, but exceptions apply, such as legal privilege protecting communications between lawyers and their clients.[306]

The right to be heard is a fundamental safeguard ensuring that the investigated person may present their side before adverse decisions are made. In Germany, the accused must be heard before any evidence is used against them in court proceedings.[307] In Finland, the right to be heard extends broadly to claims and evidence, requiring authorities to notify the investigated person before an administrative sanction is imposed or before a proposal for sanctions is submitted to the court. Finland also provides broad access rights to documents held by public authorities that may be relevant to the case.[308]

---

[299] Lassalle, (n. 2), p. 176.
[300] Blume et al., (n. 18), p. 214.
[301] *Ibid.* p. 220.
[302] *Ibid.* p. 222.
[303] *Ibid.* p. 224.
[304] Lannier, Tosza, (n. 5), p. 298.
[305] *Ibid.* p. 305.
[306] *Ibid.* p. 320.
[307] Blume et al., (n. 18), p. 214.
[308] Riekkinen, (n. 3), p. 137.

Luxembourg's legal framework formally upholds the right to be heard, requiring authorities to notify undertakings of the objections raised against them and allowing at least a month for their observations.[309] However, in practice, the right is not always fully respected in areas such as VAT enforcement, where individuals might not receive adequate notice or are refused the opportunity to respond.[310] In Ireland, the right to be heard extends to all administrative bodies when they are exercising any powers related to the administration of justice.[311]

The availability and effectiveness of remedies for investigated persons differ significantly across jurisdictions. In the Netherlands, remedies available to third parties are also accessible to investigated persons, including interim relief proceedings to challenge the relevance or nature of data obtained by administrative authorities. Dutch case law has established that individuals may challenge the inclusion of private or privileged information in the evidence obtained during investigations.[312] Similarly, in Germany, remedies for investigated persons align with those available to third parties. In Luxembourg, VAT-related cases allow for administrative or judicial complaints to be filed with the civil tribunal. However, issues arise regarding the lack of legal personality of the tax authority, complicating the process.[313] In contrast, France follows a different approach, where individuals cannot challenge the legality of investigatory measures until the information obtained is used as evidence against them. French case law permits affected persons to sue the state in cases of serious misconduct. However, the lack of immediate recourse during the investigative phase limits procedural safeguards and oversight.[314] In contrast, Irish law provides a statutory right of appeal from most administrative authorities.[315]

5. TRANSFER AND ADMISSIBILITY OF DATA OBTAINED FROM ADMINISTRATIVE INVESTIGATION POWERS

This section examines the legal frameworks governing the transfer and admissibility of electronic evidence obtained by administrative authorities from OSPs across the studied jurisdictions. The comparative analysis reveals a fragmented and often underdeveloped regulatory landscape, where sector-specific rules, informal cooperation mechanisms, and general administrative principles coexist with limited harmonisation. While most jurisdictions

[309] Lannier, Tosza, (n. 5), p. 305.
[310] *Ibid.* p. 319.
[311] Ni Loideain, (n. 12), p. 249.
[312] De Vries et al., (n. 1), p. 352.
[313] Lannier, Tosza, (n. 5), p. 304.
[314] Lassalle, (n. 2), p. 193.
[315] Ni Loideain, (n. 12), p. 249.

adhere to the principle of free evaluation of evidence, the admissibility of data gathered from third parties is subject to varying degrees of procedural safeguards, particularly when such data is transferred between administrative and criminal proceedings or across borders. The section highlights significant disparities in the availability of enforcement mechanisms, the protection of fundamental rights, and the legal certainty afforded to both investigated persons and third parties. These findings underscore the pressing need for clearer, more coherent standards to ensure the effective and accountable use of electronic evidence in administrative punitive enforcement.

5.1. The transfer of data obtained from third parties

In all studied countries, there are no specific rules on the transfer of data obtained from third parties, notably OSPs. The research identified diverse legal bases concerning transfer of evidence between proceedings. The rules governing the sharing of data vary widely depending on the authority involved, the sector in question, and the intended purpose of the transfer.

5.1.1. Transfer of evidence at national level

One of the key concerns regarding the transfer of evidence at the national level is the close interaction between administrative and criminal proceedings, leading to potential risks of circumventing the procedural safeguards specific to criminal investigations. In most jurisdictions, there is no general framework governing these transfers. Luxembourg has a legal framework for inter-administrative and judicial cooperation, though it primarily concerns customs and tax administrations.[316] Nevertheless, some similar rules can be found in several investigated countries among diverse sectors.

The existence and scope of official secrecy for administrative authorities vary across jurisdictions, with some countries imposing stricter confidentiality rules than others. In the Netherlands, tax secrecy is particularly stringent, restricting the disclosure of tax-related data solely for tax collection purposes—even preventing access by courts.[317] Similarly, Dutch financial and competition regulators are prohibited from repurposing confidential information gathered in the course of their duties.[318] Luxembourg extends tax secrecy even further, applying it beyond customs authorities to all public bodies[319] and explicitly preventing the Competition Authority from accessing tax-protected information, whether from judicial authorities or domestic and

[316] Lannier, Tosza, (n. 5), p. 325.
[317] De Vries et al., (n. 1), p. 366.
[318] *Ibid.* pp. 366-367.
[319] Lannier, Tosza, (n. 5), p. 326.

foreign tax administrations.[320] More generally, Luxembourg upholds official secrecy as a default rule across various sectors, including banking, financial markets, and competition.[321] By contrast, Finland takes a more flexible approach, allowing customs authorities to transfer information to the tax administration and police when necessary.[322] Similarly, Belgium has adopted a very flexible approach, allowing competition, financial institutions, data protection, and VAT authorities to share confidential information with other designated national administrative bodies.[323] By transferring this information, the obligation of professional secrecy is also transferred.

Across jurisdictions, exceptions to official secrecy enabling data transfers are common, but their scope and legal clarity vary significantly. Some countries, like the Netherlands[324] and Germany,[325] adopt a more restrictive and formalised approach: data may only be shared when explicitly required by law or justified by necessity and proportionality, such as for criminal investigations or judicial cooperation. In contrast, France[326] and Finland[327] allow broader inter-agency data sharing, with France explicitly excluding secrecy obligations for certain authorities and Finland mandating cooperation with tax and financial regulators. Meanwhile, Italy[328] and Belgium[329] lack clear statutory rules and instead rely on Memorandums of Understanding to facilitate cooperation, reflecting a more ad hoc and potentially less transparent model.

Some jurisdictions impose stricter rules on data transfer, particularly by limiting the purposes for which transferred data may be used. In Belgium, cooperation in competition matters requires a formal agreement enshrined in a royal decree, such as with the Belgian Institute for Postal Services and Telecommunications.[330] Finland also restricts the competition authority's ability to transfer data, permitting it only for judicial authorities, tax administration, and financial regulators, and even then, only within the narrow scope of electricity and natural gas supply supervision.[331] Luxembourg enforces strict purpose limitations in the financial sector,

[320] *Ibid.* p. 331.
[321] *Ibid.* pp. 316, 320.
[322] Riekkinen, (n. 3), p. 159.
[323] Franssen, Vandormael, (n. 6), pp. 94-95.
[324] De Vries et al., (n. 1), pp. 366-367.
[325] Blume et al., (n. 18), pp. 236, 329-340.
[326] Lassalle, (n. 2), p. 194.
[327] Riekkinen, (n. 3), p. 159.
[328] Lasagni, (n. 17), pp. 287, 290.
[329] Franssen, Vandormael, (n. 6), p. 94.
[330] *Ibid.* p. 95.
[331] Riekkinen, (n. 3), p. 160.

prohibiting further use of transferred data unless explicit consent is obtained.[332]

Rules governing data transfers between administrative and criminal authorities vary widely across jurisdictions, reflecting different balances between enforcement efficiency and procedural safeguards. Some countries, like France[333] and Luxembourg,[334] impose a legal duty on administrative bodies to report suspected criminal offences and transfer relevant data to judicial authorities, ensuring systematic cooperation. Others, such as Finland[335] and Ireland,[336] adopt a more discretionary model, where reporting is optional or based on voluntary cooperation. Belgium presents a mixed approach: while VAT authorities routinely share data with prosecutors,[337] other bodies like competition and data protection authorities rely on informal practices, often contingent on prosecutorial willingness.[338] Germany and Italy take a more restrictive stance, requiring that data transfers meet specific legal thresholds—Germany limits transfers to cases involving distinct offences,[339] while Italy mandates compliance with criminal procedure rules and evidentiary safeguards.[340]

The transfer of data from judicial to administrative authorities is permitted in all studied jurisdictions, but the conditions and safeguards vary considerably. Some countries, like the Netherlands and Italy, allow such transfers under strict procedural conditions: Dutch courts permit the use of criminal evidence in administrative proceedings if judicial oversight is ensured—a practice upheld by the ECtHR[341] but controversial among scholars—[342] while Italy requires compliance with the double-proportionality test established by the ECJ, despite lacking explicit national rules.[343] France[344] and Luxembourg adopt sector-specific approaches, granting prosecutors discretion to share data, though Luxembourg requires judicial authorisation when criminal investigations are ongoing.[345] Germany applies

[332] Lannier, Tosza, (n. 5), p. 327.
[333] Lassalle, (n. 2), p. 195.
[334] Lannier, Tosza, (n. 5), p. 327.
[335] Riekkinen, (n. 3), p. 159.
[336] Ni Loideain, (n. 12), p. 264.
[337] Franssen, Vandormael, (n. 6), p. 97.
[338] *Ibid.* pp. 94, 97.
[339] Blume et al., (n. 18), p. 239.
[340] Lasagni, (n. 17), pp. 288-291.
[341] ECtHR, *Janssen de Jong Groep B.V. and Others v. the Netherlands*, 16.05.2023, no. 2800/16 (referred to the Grand Chamber); ECtHR, *Burando Holding B.V. and Port Invest B.V. v. the Netherlands*, 16.05.2023, no. 3124/16 and 3205/16.
[342] De Vries et al., (n. 1), pp. 368-370.
[343] Lasagni, (n. 17), pp. 288.
[344] Lassalle, (n. 2), p. 194.
[345] Lannier, Tosza, (n. 5), p. 327.

consistent safeguards for both directions of data exchange, ensuring legal symmetry.[346] In contrast, Finland and Belgium impose stricter controls: Finland mandates the destruction of surplus judicial data unless explicitly authorised for administrative use,[347] and Belgium requires prior approval from judicial authorities for transfers involving ongoing criminal procedures.[348]

5.1.2. Transfer of evidence at international level

EU law offers many specific rules on administrative cooperation at supranational level.[349] Overall, these legislative acts limit grounds for refusal when transferring data within the EU for administrative cooperation. However, at national level, rules on transfer of evidence at international level remain very diverse.

International data transfers by administrative authorities are governed by diverse national rules, reflecting varying levels of restrictiveness and legal clarity. Countries like the Netherlands[350] and Germany[351] adopt a formal and cautious approach: transfers are only allowed to foreign authorities

[346] Blume et al., (n. 18), p. 240.
[347] Riekkinen, (n. 3), p. 161.
[348] Franssen, Vandormael, (n. 6), p. 96.
[349] See, for instance, Council Regulation (EC) no. 515/97 of 13.03.1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, Article 4; Regulation (EU) no. 952/2013 of the European Parliament and of the Council of 09.10.2013 laying down the Union Customs Code, Article 47; Regulation (EU) no. 596/2014 of the European Parliament and of the Council of 16.04.2014 on market abuse, Articles 25 and 26; Regulation (EU) 2016/1011 of the European Parliament and of the Council of 08.06.2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds, Article 39; Council Regulation (EC) no. 1/2003 of 16.12.2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, Article 12; GDPR, Article 61; Directive (EU) 2019/1 of the European Parliament and of the Council of 11.12.2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, Article 24; Directive (EU) 2016/680 of the European Parliament and of the Council of 27.04.2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, Article 50; Council Regulation (EU) no. 904/2010 of 07.10.2010 on administrative cooperation and combating fraud in the field of value added tax; Council Directive 2010/24/EU of 16.03.2010 concerning mutual assistance for the recovery of claims relating to taxes, duties and other measures; Council Directive 2011/16/EU of 15.02.2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EE.
[350] De Vries et al., (n. 1), p. 370.
[351] Blume et al., (n. 18), p. 241.

performing comparable functions, often requiring explicit authorisation or court orders. Finland similarly limits transfers through a strict purpose limitation principle.[352] Luxembourg and France follow sector-specific models, with Luxembourg imposing stringent confidentiality and use restrictions—especially in financial and customs matters[353]—while France allows exchanges based on reciprocity and functional equivalence.[354] Belgium permits broader sharing under competition law but faces practical constraints due to professional secrecy and procedural inconsistencies.[355] At the other end of the spectrum, Ireland lacks a binding legal framework and relies on non-binding Memorandums of Understanding, offering flexibility but less legal certainty.[356]

5.2. The admissibility of data obtained from third parties

In most jurisdictions, there are no specific rules governing the admissibility of data obtained from third parties, meaning that general rules of evidence apply. Administrative proceedings across various countries generally follow the principle of free evaluation of evidence, according to which any information may be used as proof unless it is manifestly improper or obtained in violation of fundamental rights (NL,[357] FR,[358] GE,[359] FI,[360] BE,[361] LU[362], IT[363], PL[364]). As literature and case law regarding admissibility of evidence gathered in administrative proceedings is limited, many countries refer to criminal procedure standards.

Admissibility of evidence in administrative proceedings is generally governed by broad principles, but national approaches differ in how strictly they apply safeguards. The Netherlands and Germany apply nuanced balancing tests: Dutch courts may exclude evidence that violates fundamental rights or lacks proportionality,[365] while German courts assess whether the state's interest in prosecution outweighs individual rights and only admit transferred evidence if it could have been lawfully obtained in the receiving

[352] Riekkinen, (n. 3), p. 165.
[353] Lannier, Tosza, (n. 5), p. 329.
[354] Lassalle, (n. 2), pp. 175-176.
[355] Franssen, Vandormael, (n. 6), p. 95.
[356] Ni Loideain, (n. 12), p. 265.
[357] De Vries et al., (n. 1), p. 372.
[358] Lassalle, (n. 2), p. 196.
[359] Blume et al., (n. 18), p. 241.
[360] Riekkinen, (n. 3), p. 163.
[361] Franssen, Vandormael, (n. 6), p. 102.
[362] Lannier, Tosza, (n. 5), p. 331.
[363] Lasagni, (n. 17), p. 292.
[364] Kaszubowski, Steinborn, (n. 26), p. 394.
[365] De Vries et al., (n. 1), pp. 349-351, 372.

proceeding.[366] France, by contrast, exercises limited judicial scrutiny over admissibility.[367] Finland and Belgium adopt stricter standards in administrative contexts, with Finnish authorities barred from using evidence that would be inadmissible on appeal,[368] and Belgian regulators—especially in data protection and finance—applying cautious, criminal-law-inspired standards.[369] Luxembourg and Italy take a more procedural approach: Luxembourg requires legal acquisition and proper communication,[370] while Italian authorities assess admissibility case by case.[371]

Sector-specific regulations may impose broad admissibility conditions. In Belgium, competition law explicitly allows various forms of evidence, such as documents, electronic messages, and recordings, but evidence is inadmissible if formal conditions are not met, reliability is compromised, or its use contravenes the right to a fair trial.[372] In contrast, rules on admissibility of evidence are not expressly provided by banking law, financial markets law, and data protection law, they apply, voluntarily, rules on criminal procedures by analogy.[373] Similarly, Luxembourg's competition authority accepts a wide range of evidence, and information obtained is generally admissible unless controlled by specific procedural requirements, and the VAT authority admits evidence based on the records of its agents.[374]

When it comes to international data transfers, Dutch administrative authorities must verify that the foreign authority providing the data maintains an equivalent level of rights protection, ensuring compliance with fair trial principles.[375] However, they are not required to verify the legality of how the data was obtained by the foreign authority, as this responsibility rests with the originating jurisdiction.[376] Differently, the German Federal Court of Justice, in Encrochat decision, has further listed exhaustive reasons for declaring evidence inadmissible following an international transfer in criminal proceedings, which might be later transposed to administrative cooperation.[377]

---

[366] Blume et al., (n. 18), p. 242.
[367] Lassalle, (n. 2), p. 196.
[368] Riekkinen, (n. 3), pp. 164-166.
[369] Franssen, Vandormael, (n. 6), p. 102.
[370] Lannier, Tosza, (n. 5), p. 331.
[371] Lasagni, (n. 17), p. 292.
[372] Franssen, Vandormael, (n. 6), p. 102.
[373] *Ibid.* p. 103.
[374] Lannier, Tosza, (n. 5), p. 331.
[375] De Vries et al., (n. 1), 372.
[376] *Ibid.* p. 374.
[377] Blume et al., (n. 18), p. 243. The reasons are the following: violations of principles of international law, for instance, a violation of the sovereignty of another state; violations of the *ordre public*, especially of fundamental principles regarding the rule of law; violations of

6. CONCLUSIONS

The preceding analysis reveals a landscape where, despite the increasing digitisation of society, administrative authorities have so far demonstrated a limited appetite for gathering electronic evidence from third parties, particularly online service providers (OSPs), often preferring traditional gathering evidence from persons concerned by the investigation. However, this approach is beginning to evolve, with a growing recognition of the potential and necessity of leveraging electronic evidence in administrative enforcement across various jurisdictions.

The study revealed structural variations in administrative punitive enforcement, with some countries clearly separating administrative and criminal proceedings while others operate under dual systems or blended approaches. Furthermore, the lines between supervisory and investigative functions within administrative enforcement are often blurred. Importantly, there is a growing acknowledgement that many administrative punitive proceedings possess a 'criminal nature' under the jurisprudence of the ECtHR, necessitating the application of enhanced procedural safeguards.

The legislative frameworks governing administrative investigations present a contrast between comprehensive general laws and fragmented sector-specific regulations. Administrative authorities generally possess both specific and general powers to gather data from third parties, including OSPs, though the categories of addressees, the types of data accessible, and the conditions for requesting this information differ significantly across countries and sectors. What has been clearly demonstrated is that the laws offer abundant opportunities to request data from persons concerned, but those laws either do not apply or oftentimes it is unclear whether they apply to third parties (e.g., the OSPs). Their open formulation, however, on many occasions offer the possibility for them to be used to request data from third parties.

While foundational legal principles such as proportionality and the right to be heard underpin these proceedings, their specific application and protection vary. Notably, safeguards towards third parties subject to these data requests are limited and inconsistent, which can be explained by the fact that they are usually not written having in mind such data requests. This raises concerns about legal certainty and the protection of fundamental rights.

The transfer of data obtained through administrative investigation powers, both at national and international levels, relies mostly on general principles of cooperation and often varies significantly depending on the authorities and sectors concerned. Similarly, the admissibility of such data is

---

provisions of the law of mutual assistance that protect individual rights; violations of provisions of the constitution, especially an encroachment on fundamental rights; and violations of specific provisions in procedural law.

largely governed by the principle of free evaluation of evidence, with many jurisdictions drawing analogies from criminal procedure in the absence of specific administrative law precedents.

In conclusion, this research reveals that administrative punitive enforcement, at least in its legal framework and practice, seems to be less advanced in recognising the potential and need for electronic evidence, contrary to criminal enforcement.[378] The research demonstrates that there is a noticeable lag in the comprehensive regulation of data access, particularly concerning information held by third parties in administrative proceedings, hence showing a need to adapt to the challenges of adapting to the digital age. The limited and inconsistent guarantees and remedies available to both third parties and the investigated person underscore the need for further reflection and the development of clearer legal standards at the crossroad of administrative and criminal law.

[378] See a comprehensive analysis in V. Franssen, S. Tosza (eds.), *The Cambridge Handbook of Digital Evidence in Criminal* University Press, 2025.