14. POLICY RECOMMENDATIONS

S. TOSZA and S. LANNIER

1. INTRODUCTION

The ELEVADMIN project addresses a critical gap in the understanding of how electronic evidence can be gathered in administrative punitive investigations. While the use of such evidence has been extensively studied in the context of criminal law, administrative enforcement—particularly at the EU level and within Member States—has remained underexplored. The project investigates the legal bases, practical mechanisms, and institutional capacities for requesting electronic evidence from Online Service Providers (OSPs), with a particular focus on the role of the European Anti-Fraud Office (OLAF). It aims to assess the feasibility and implications of extending OLAF's powers in this domain, while ensuring compliance with fundamental rights and procedural safeguards.

The research undertook a comprehensive comparative analysis across nine EU Member States—Belgium, Finland, France, Germany, Ireland, Italy, Luxembourg, the Netherlands, and Poland—and at the EU level. It focused on five key areas of punitive administrative enforcement: customs, Value Added Tax (VAT), competition law, General Data Protection Regulation (GDPR) enforcement, and financial market supervision. These domains were selected for their relevance to the protection of the EU's financial interests and their varying degrees of interaction between administrative and criminal enforcement.

The comparative chapter reveals a fragmented and evolving legal landscape across nine EU Member States. While administrative authorities increasingly recognise the value of electronic evidence, particularly from OSPs, their powers to obtain such data remain inconsistent and often ambiguous. The study identifies a patchwork of specific and general legal bases, with significant variation in the scope of powers, categories of accessible data, procedural safeguards, and enforcement mechanisms. Notably, administrative frameworks often lack explicit procedural safeguards, prompting administrative courts to rely on overarching constitutional principles or general norms of administrative law to fill the gaps. The admissibility and transfer of electronic evidence—especially across

administrative and criminal domains—lack consistent specific standards, aside the general principle of the freedom of proof.

At EU level, the Directorate-General for Competition of the European Commission (DG COMP), the European Central Bank (ECB), and European Securities and Markets Authority (ESMA) possess extensive investigatory powers in their respective domains—competition law, banking supervision, and financial markets. Yet, there is a notable absence of explicit legal bases allowing them to request electronic evidence directly from OSPs. DG COMP and the ECB rely on broadly framed general powers to request any information (i.e., any kind of data), but their applicability to OSPs remains uncertain or limited by personal scope (e.g., ECB's powers are confined to supervised entities and their business partners). ESMA, by contrast, it is specifically allowed to request telephone and data traffic records, though, as for the ECB, only from supervised entities. Across all three authorities, the use of such powers in practice remains rare, with investigations typically relying on data obtained directly from the entities under investigation.

2. GENERAL RECOMMENDATIONS AS TO GATHERING OF ELECTRONIC EVIDENCE FROM OSPS IN PUNITIVE ADMINISTRATIVE PROCEEDINGS

These findings underscore the urgent need for clearer, more coherent legal frameworks to ensure effective, fundamental rights-compliant administrative enforcement in the digital age. First, a clear legal basis should be established—preferably at the EU level—to define when and how administrative authorities may access electronic evidence from third parties, particularly OSPs, including the types of data and applicable conditions. Second, procedural safeguards must be introduced for third parties, including to certain extent to the OSPs, by formalising data requests as administrative decisions and ensuring transparency, the right to be heard, and access to remedies. Third, intrusive data requests—especially those involving sensitive data—should be subject to prior authorisation by an independent or judicial authority, in line with European Court of Human Rights (ECtHR) and European Court of Justice (ECJ) case law, to uphold fundamental rights and ensure proportionality. Finally, the admissibility and transfer of electronic evidence between administrative and criminal proceedings must be clarified to prevent circumvention of safeguards and ensure legal coherence, particularly through the application of the purpose limitation principle.

Recommendation no. 1: Establish a Clear Legal Basis for Access to Electronic Evidence by Administrative Authorities

Many jurisdictions rely on general or ambiguously framed powers. A harmonised EU-level framework could define when and how administrative

authorities can request electronic evidence from OSPs, specifying the types of data (e.g., subscriber, traffic, content) and applicable conditions. In the absence of EU-level framework, Member States should ensure consistency among areas of enforcement, which could foster legal clarity around administrative investigations regimes. In particular, Member States could rely on EU definitions regarding typologies of OSPs and data, to ensure consistency between national and EU legislation. Also, Member States should clarify whether such a clear legal basis would be available under the supervision or investigation competences of administrative authorities, especially given that the distinction between these procedural stages remains blurred, or entirely absent, in many of the jurisdictions analysed.

Recommendation no. 2: Recognise Data Requests as Administrative Decisions with Procedural Safeguards

In many Member States, data requests issued by administrative authorities, particularly to third parties such as OSPs, are not formally recognised as administrative decisions. Instead, they are often treated as preliminary investigative steps, which results in the absence of procedural safeguards for both affected individuals and the addressees. This lack of formal recognition undermines transparency, legal certainty, and the protection of fundamental rights. To address this gap, legislation and judicial authorities should explicitly classify data requests as administrative acts or decisions. This would trigger the application, for the investigated person, of existing procedural safeguards, including the right to be notified (once it no longer jeopardises the investigation), the right to be heard, and access to effective remedies against data requests. While some safeguards may be inferred from general constitutional or administrative principles, most administrative frameworks lack detailed provisions governing the procedural aspects of data requests. These include provisions on the requirement of a reasoned decision, designation of the competent authority, notification procedures, and effective remedies. At a minimum, data requests should comply with the procedural guarantees enshrined in the GDPR.

Moreover, some safeguards should extend to third parties, such as OSPs, who are not the primary subjects of the investigation, but are instrumental for its execution. In many jurisdictions, OSPs can only challenge a data request once a sanction is imposed for non-compliance. However, such sanctions are not uniformly available across sectors, and where they exist, they vary significantly in scope and severity. This fragmented approach leaves OSPs without meaningful recourse in many cases, unless the OSP chooses to oppose the request and face a risk of a sanction. Such recognition is particularly important when the requested data may implicate the OSP itself, for example, in cases involving potential breaches of data protection, where

the principle against self-incrimination must be respected. To ensure proportionality and legality, third parties should be informed of the purpose and legal basis of the data request. This is particularly crucial when the data was originally retained for a specific purpose (e.g., investigation of serious crime), as the ECJ has repeatedly held that access to data must meet an equivalent threshold of seriousness (e.g., when it regards violations to administrative law or investigation of crimes by administrative authorities).[1]

Finally, administrative and criminal investigative competences are often blurred or explicitly overlapping, particularly in systems where law enforcement authorities, whether administrative or criminal, can determine the most appropriate procedural route. This fluidity between enforcement regimes must not result in the erosion of criminal procedural safeguards. Therefore, it is essential to ensure that third parties, such as OSPs, have access to remedies to a similar degree as in criminal cases, especially when the investigation may ultimately lead to criminal proceedings.

Recommendation no. 3: Require Independent or Judicial Oversight for Intrusive Data Requests

To align with ECtHR and ECJ jurisprudence, particularly in cases involving data that may reveal 'precise conclusions on the private lives of the persons'[2] (e.g., traffic or content data), requests should be subject to prior authorisation by a judicial or independent authority, especially when the data is not held by the investigated person. In particular, the scope of data requests must be clarified, as outlined in Recommendation no. 1, to ensure that data requiring judicial authorisation under criminal law is afforded equivalent protection in administrative proceedings. This is especially relevant in hybrid enforcement contexts, where administrative sanctions may qualify as criminal in nature under the ECtHR's *Engel* criteria,[3] or where administrative investigations may lead to or run parallel with criminal proceedings. Judicial or independent oversight serves as a critical safeguard to assess the necessity and proportionality of the measure, especially in light of the sensitivity of the data and the potential impact on fundamental rights, including the right to privacy, data protection, and due process. The principle of proportionality

[1] ECJ, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, 21.12.2016, C-203/15 and C-698/15, §115; ECJ, *A.G. v. Lietuvos Respublikos generalinė prokuratūra*, 07..09.2023, C-162/22, §43; ECJ, *La Quadrature du Net and Others v. Premier ministre and Ministère de la Culture*, 30.04.2024, C-470/21, §§95-122.

[2] ECJ, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 08.04.2014, C-293/12 and C-594/12.

[3] ECtHR, *Engel and Others v. the Netherlands*, 08.06.1976, no. 48272/17, 57479/17, 510/18, 7936/18, 27115/18.

should guide the assessment of whether the purpose of the data request justifies the level of intrusion, ensuring that access to sensitive data is reserved for cases of sufficient gravity and legal clarity.

Recommendation no. 4: Clarify the Admissibility and Transfer of Evidence Between Proceedings

In the evolving landscape of EU enforcement, where administrative and criminal investigations increasingly intersect, the ability to transfer evidence, including electronic evidence, between proceedings is not merely a procedural convenience—it is a structural necessity. Rules should be adopted to regulate the transfer of evidence between administrative and criminal proceedings, ensuring that such transfers do not circumvent procedural safeguards and that evidence remains admissible under both frameworks. So far, much attention has been dedicated to international cooperation in the criminal justice system, on one side, and in administrative cooperation, on the other side. For instance, despite administrative sovereignty over taxation, the increasing mobility of taxpayers, the growth in cross-border transactions, as well as the internationalisation of financial instruments have led to develop in-depth administrative cooperation among their tax authorities through the cross-border framework and instruments provided at the EU level. Yet, little attention has been dedicated to the transfer of evidence gathered in administrative proceedings towards criminal proceedings.

In particular, Member States should apply the principle of purpose limitation when assessing the permissibility of transferring data gathered from third parties. This principle, rooted in ECJ case law on data retention and access, requires that data collected for one purpose, especially a serious one such as criminal investigation, should not be repurposed for a less serious objective, such as administrative violations. In legal systems where the boundaries between supervision, punitive administrative proceedings, and criminal investigations are often blurred or overlapping, the original purpose for which the data was collected must guide both the permissibility of its transfer (especially from criminal to administrative proceedings) and the procedural safeguards that should be triggered upon transfer (particularly from administrative to criminal proceedings). Ensuring that the seriousness of the investigative purpose aligns with the sensitivity of the data is essential to uphold the principle of proportionality and to protect fundamental rights.

3. Gathering of electronic evidence from OSPs by OLAF

While national and EU administrative authorities play a vital role in enforcing compliance and investigating irregularities, they face significant limitations in addressing the increasingly complex and transnational nature of

fraud affecting the EU budget. The digitalisation of illicit practices, the use of sophisticated concealment techniques, and the cross-border dimension of financial misconduct demand a coordinated and specialised response at the EU level. OLAF occupies a unique position in this landscape. It is tasked with protecting the financial interests of the EU through independent administrative investigations, particularly in contexts where national authorities lack jurisdiction, capacity, or incentive to act. OLAF's mandate is especially critical in cases involving internal EU institutions,[4] non-participating Member States to the European Public Prosecutor's Office (EPPO),[5] third countries,[6] or when the EPPO declines to open an investigation.[7] In these scenarios, OLAF serves as the EU's primary investigative body, and its effectiveness directly impacts the integrity of the EU budget. As fraud and irregularities evolve in tandem with digital technologies, OLAF must be equipped with tools that match the sophistication of the threats it faces.

OLAF's investigative powers have gradually expanded to reflect the changing nature of fraud and the growing importance of digital evidence. Recent reforms have introduced new capabilities, such as the power to request bank account information[8] and to inspect privately owned devices used for professional purposes.[9] These developments mark a shift toward investigative techniques traditionally associated with criminal proceedings, underscoring OLAF's need to operate in a fast-paced, technologically advanced environment. However, OLAF remains institutionally distinct from criminal law enforcement bodies like the EPPO. While the EPPO Regulation does not

[4] Article 4 OLAF Regulation, Regulation (EU, Euratom) no. 883/2013 of the European Parliament and of the Council of 11.09.2013 concerning investigations conducted by the European Anti-Fraud Office.

[5] The EPPO was established under enhanced cooperation. According to Article 86 Treaty on the Functioning of the EU, in the absence of unanimity in the Council, a group of at least nine Member States may establish enhanced cooperation on the basis of the draft regulation concerned. The EPPO Regulation was adopted in October 2017 by 22 out of 27 Member States. Currently, Hungary, Ireland and Denmark are not taking part in enhanced cooperation, while Poland and Sweden have recently decided to join. See Council Regulation (EU) 2017/1939 of 12.10.2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office.

[6] Even if the EPPO has recently considered to be competent over criminal offences related to European Union funds allocated to third countries. Concretely and considering the seat of EU Institutions, bodies, offices and agencies (IBOAs) involved in expenditure, both Belgian and Luxembourgish criminal laws confirm that an offence is considered as having been committed on their territory whenever any constituent element of the criminal offence has taken place on their territory.

[7] Article 12e OLAF Regulation and Article 101(3) EPPO Regulation.

[8] Article 7(3) OLAF Regulation.

[9] Article 3(5) and 4(2) OLAF Regulation.

explicitly address electronic evidence in general,[10] European Delegated Prosecutors (EDPs) can rely on national criminal procedure laws to request such data.[11] OLAF, by contrast, lacks a comparable legal basis or practice for directly requesting electronic evidence from OSPs, placing it at a disadvantage in investigations in certain sectors that increasingly hinge on digital traces.

Despite its central role in safeguarding EU financial interests, OLAF currently does not possess the power to directly request electronic evidence—a gap that significantly undermines its investigative capacity. The ability to access subscriber data, traffic records, or content data held both by investigated persons and by third parties, including OSPs, is essential for uncovering hidden arrangements, identifying accomplices, and demonstrating the organised nature or intent behind fraudulent schemes. So far, OLAF has to rely on indirect and less straightforward mechanisms such as on-the-spot checks or general requests for information to obtain data from third parties. While OLAF's powers have evolved—particularly through the 2020 reform introducing a general duty of cooperation and enhanced procedural safeguards—its investigatory tools remain limited by the absence of coercive powers and enforceable mechanisms. Additionally, the fragmented nature of OLAF's legal framework, which combines EU regulations, internal guidelines, and national law, often results in legal uncertainty. Moreover, the admissibility of OLAF-collected evidence in national or EPPO proceedings depends on whether they act within their own framework under a complementary investigation or in support to an ongoing investigation at EPPO or national level. While in the latter OLAF must comply with the legal framework of the supported investigation, transfer of evidence following a complementary investigation raises challenges regarding compliance with national evidentiary standards and fundamental rights, and concerns about the effectiveness and legal robustness of OLAF's investigative outputs.

As digital evidence becomes indispensable in both administrative and criminal investigations, OLAF must be empowered to gather such data under clearly defined conditions and safeguards. The study underpinning this book highlights the feasibility of establishing a system analogous to OLAF's access to bank accounts, potentially supported by national anti-fraud coordination services and judicial oversight. Moreover, given OLAF's role in transmitting evidence to criminal authorities like the EPPO, and *vice versa*, it is crucial to regulate the admissibility and transfer of electronic evidence between

[10] Council Regulation (EU) 2017/1939 of 12.10.2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office. Article 30(1)e however address interception of communications.
[11] Article 30(4) EPPO Regulation.

proceedings. Without such powers and frameworks, OLAF risks falling behind in the digital age, unable to meet the demands of modern fraud detection and enforcement.

4. RECOMMENDATIONS WITHIN THE CURRENT LEGISLATIVE FRAMEWORK OF OLAF

In the absence of legislative reform, OLAF can still enhance its operational effectiveness through the following measures:

Recommendation no. 5: Leverage National Legal Frameworks via Cooperation

OLAF should strengthen collaboration with national anti-fraud coordination services (AFCOS) to access electronic evidence indirectly, relying on national authorities' powers under domestic law. This would require formalised cooperation protocols and possibly judicial assistance at the national level. In particular, OLAF could seek judicial validation of especially intrusive data requests through national courts, thereby reinforcing the legitimacy and admissibility of such evidence in subsequent proceedings. However, OLAF may encounter difficulties in relying on national investigative powers, as administrative punitive frameworks vary significantly across sectors and Member States. Depending on the type of fraud or irregularity, national authorities may not possess equivalent powers to request electronic evidence, which limits OLAF's ability to access relevant data through cooperation mechanisms.

Recommendation no. 6: Develop Internal Guidelines for Voluntary Cooperation with OSPs

OLAF should establish a structured and transparent framework for requesting data from OSPs on a voluntary basis, particularly in the absence of a dedicated legal basis. Such a framework should promote consistency across investigations, ensure compliance with fundamental rights, and foster trust with private actors who may hold relevant electronic evidence. This approach should include standardised request templates, internal review procedures, technical protocols for secure data transfer, and safeguards for both investigated persons and third parties. These guidelines should be adopted pursuant to Article 17(8) of the OLAF Regulation, which empowers OLAF to develop internal rules governing its investigative practices. While non-binding, such guidelines would serve as a harmonising tool to guide OLAF's operational behaviour and signal its commitment to legal certainty and rights protection. They would also help clarify OLAF's expectations and

procedures for OSPs, encouraging cooperation in cases where formal powers are lacking.

In parallel, OLAF should continue to strengthen its technical capacity in digital investigations. This includes targeted training in open-source intelligence (OSINT), blockchain analytics, and metadata interpretation, as well as the development of internal expertise in emerging technologies. In doing so, OLAF should ensure that its practices align with the data protection framework, including the GDPR and the Artificial Intelligence Act.[12] This alignment is essential to ensure that voluntarily obtained data is handled lawfully, ethically, and in a manner that supports its admissibility in follow-up proceedings.

Recommendation no. 7: Enhance Evidence Transfer Mechanisms

The current fragmentation between administrative and criminal frameworks, particularly in the context of digital evidence, risks undermining both the effectiveness of investigations and the protection of fundamental rights. This is especially relevant for OLAF, whose administrative findings often serve as the basis for criminal prosecutions, notably by the EPPO. Given the close interconnection between OLAF's administrative investigations and subsequent criminal prosecutions, whether at the national level or through the EPPO, clarifying the rules governing evidence transfer is essential. Enhancing evidence transfer mechanisms is essential to ensure the operational continuity between OLAF and criminal enforcement bodies like the EPPO. OLAF should formalise procedures, such as through internal guidelines for the admissibility and transfer of electronic evidence between administrative and criminal proceedings, particularly with the EPPO. This includes ensuring compliance with the principle of purpose limitation and data protection rules. To that aim, guidelines should not only regard general legal principles but especially include technical rules around data transfer.

5. Recommendations to amend the legislative framework of OLAF

While OLAF can already strengthen its operational framework through internal guidelines, particular attention must be given to embedding new investigatory powers within its formal legal mandate. The following recommendations are especially timely, as the European Commission is expected to publish its evaluation report on OLAF in June 2026. This report may serve as a basis for proposing amendments to the OLAF Regulation, including updates to its investigative powers to reflect the evolving nature of

[12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13.06.2024 laying down harmonised rules on artificial intelligence.

fraud and irregularities affecting the EU's financial interests. Anticipating this reform process, it is essential to identify concrete legislative improvements that would enhance OLAF's ability to gather electronic evidence in a manner that is both effective and compliant with fundamental rights.

Recommendation no. 8: Introduce a Specific Legal Basis for Accessing Electronic Evidence from OSPs

OLAF's founding regulation should explicitly authorise the Office to request electronic evidence from OSPs, including subscriber, traffic, and content data, under clearly defined conditions. Such a reform should specify the categories of data OLAF may request, the circumstances under which such requests are justified, particularly under which proceedings, depending on the seriousness of the violation under investigation, and the procedural rights of data subjects and third parties, drawing on ECtHR and ECJ case law. In defining OSPs and data categories, the legal framework should refer to pre-existing EU definitions, to ensure consistency among sectors. In drafting such a specific legal basis, attention should be particularly drawn to consistency with the E-evidence Regulation.[13]

Recommendation no. 9: Define Procedural Safeguards and Oversight Mechanisms

Should this power be introduced, it would represent a significant expansion of OLAF's investigative reach into areas traditionally governed by criminal procedure. As such, it must be framed within a legal architecture that ensures compliance with the European Convention on Human Rights, the Charter of Fundamental Rights of the EU, and relevant case law of the ECtHR and the ECJ. In particular, requests for data should be classified as administrative decisions, thereby triggering procedural safeguards under EU and national administrative law for investigated persons. Data subjects, when appropriate, should be informed of the request and given an opportunity to contest it, unless secrecy is justified by the needs of the investigation. OSPs should be granted a minimum set of procedural safeguards, particularly in situations where data requests may implicate them directly or risk infringing the principle against self-incrimination. Minimal procedural safeguards are essential to ensure access to remedies and to uphold fundamental rights, especially in contexts where the boundaries between OLAF's administrative investigations and EPPO-led or national criminal proceedings are blurred.

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

Creating procedural protections for OSPs helps ensure that administrative processes do not inadvertently bypass the safeguards required in criminal investigations. For intrusive data types (e.g., traffic or content data), prior authorisation by a judicial or independent authority should be mandatory. Each request should be subject to a documented assessment of its necessity and proportionality, particularly in light of the fundamental rights at stake. Affected parties should have access to effective remedies, including the right to challenge the legality of the request and the use of the data obtained.

Recommendation no. 10: Enable Cross-Border Enforcement and Mutual Recognition

OLAF should be allowed to issue data access requests that are recognised across Member States, adapted for administrative investigations. As administrative punitive proceedings do not result in penalties as severe as those in criminal proceedings, such as deprivation of liberty, cross-border cooperation mechanisms in this domain should be designed with greater flexibility than those used under criminal cooperation frameworks. However, this flexibility must be balanced with appropriate safeguards, particularly given the diversity and overlap of competences between administrative and criminal enforcement at the EU level. In cases where an administrative investigation may lead to, or run parallel with, criminal proceedings, safeguards must be in place to ensure that the procedural rights applicable in criminal contexts are not undermined. This includes ensuring that data obtained through cross-border administrative cooperation is subject to adequate legal scrutiny and that its use in subsequent criminal proceedings respects the principles of legality, proportionality, and fundamental rights protection. More generally, provisions governing the transfer of electronic evidence between OLAF and national criminal authorities and the EPPO, should ensure that such transfers respect procedural safeguards and data protection principles.