Electronic Evidence Collection in Cases of the European Public Prosecutor's Office

Legal Framework, Procedures, and Specifics

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Alexandru Frunza-Nicolescu *

ABSTRACT

Electronic evidence (e-evidence) is necessary and relevant with regard to many cases of serious, organised, or cross-border crime. This is also true for cases investigated by the European Public Prosecutor's Office (EPPO). This article outlines the current legal framework, procedures, and mechanisms available to the EPPO for the collection of e-evidence in different case scenarios. It also takes into account the requirements for the protection of personal data, in particular arising in the transfer of operational data to authorities and private parties in third countries.

AUTHOR

Alexandru Frunza-Nicolescu

Senior Legal Assistant
European Public Prosecutor's Office
(EPPO)

CITE THIS ARTICLE

Frunza-Nicolescu, A. (2023). Electronic Evidence Collection in Cases of the European Public Prosecutor's Office : Legal Framework, Procedures, and Specifics. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2023-016

Published in eucrim 2023, Vol. 18(2) pp 210 – 216

https://eucrim.eu

ISSN:

I. Introduction

The European Public Prosecutor's Office (EPPO) is the independent public prosecution office of the European Union responsible for investigating, prosecuting, and bringing to judgment crimes against the financial interests of the EU.[1] Like for any other national criminal justice authority, EPPO's success in investigating and prosecuting crime relies on the lawful, effective, and efficient collection of evidence.

The perpetrators of offences falling within EPPO's jurisdiction often make use of the Internet and information and communication technologies (ICTs) in the course of organising and committing their crimes, laundering the crime proceeds, or hiding the traces of their offences.

In general, computer data of any type or form can contain relevant traces of criminal activity. Thus, in order to prove that a crime has been committed, to identify the money laundering processes and the crime proceeds, and to bring the perpetrators to justice, the EPPO has to preserve, collect, assess, and make use of e-evidence in the investigations it carries out. Given the current architecture of the Internet and the significant number of Internet, social media, or communication services provided by companies located in foreign jurisdictions, e-evidence in many cases falls outside the territorial jurisdiction of the EPPO.[2]

Collecting cross-border e-evidence from foreign jurisdictions can be very challenging for any EU national judicial authority due to the scale and quantity of devices, users, and victims, the technical challenges like encryption or anonymisation, as well as territoriality and jurisdictional aspects.[3] Such collection requires knowledge and subsequent use of a variety of legal frameworks, procedures, cooperation networks, and technical arrangements. The structure, organisation, and legal framework of the EPPO – an EU indivisible body operating as a single office with a decentralised structure[4] – adds an additional layer of specific requirements to those already existing for traditional national criminal justice authorities.

In EPPO cases, e-evidence might be located, controlled, or stored in different jurisdictions, including: the jurisdiction of (1) the Member State of the handling[5] European Delegated Prosecutor (handling EDP); (2) the Member State of the assisting European Delegated Prosecutor (assisting EDP);[6] (3) a non-participating Member State;[7] (4) a party to the Council of Europe (CoE) Budapest Convention on Cybercrime,[8] including Denmark; (5) the EPPO non-participating Member State Ireland; and 6) any other third country not covered by scenarios one to five. In a seventh scenario, e-evidence might be controlled by foreign Internet and media service providers that can, in specific situations, share it directly with foreign criminal justice authorities on a voluntary basis, which is particularly true for providers based in the US. Each of these seven scenarios with their different rules, procedures, and mechanisms will be examined in the respective subsections of Section II. Section III. will be dedicated to the legality of transfers to third countries taking into account the relevant data protection rules in the EPPO Regulation before some concluding remarks in Section IV. The following analysis is based on the current legal framework and does not address the future legal framework on cross-border e-evidence collection following the entry into force of lined-up but not yet applicable EU and international instruments in the next few years, such as the EU e-evidence package[9] or the Second Additional Protocol to the Budapest Convention[10]. Neither will the article address in detail the issue of the competent jurisdiction over the computer data required by EPPO (i.e., questions regarding the determination of data location, storage place of data, location of the controller, location or nationality of data owner, etc.). The author rather assumes that the location of the data is established if the competent jurisdiction to be addressed by the EPPO in its request for computer data is to be considered.

https://doi.org/10.30709/eucrim-2023-016

II. Case Scenarios

1. Scenario 1: e-evidence located within the territorial jurisdiction of the handling EDP

Computer data relevant for EPPO investigations might be located in the territory of the Member State participating in the EPPO of the handling EDP. In this case, the EDP will make use of the legal provisions, procedures, and technical arrangements available at national level, similar to any other criminal justice authority from his/her state. All 22 Member States participating in the EPPO are parties to the Budapest Convention on Cybercrime and have implemented the relevant provisions of the Convention in their criminal procedural law, thus insuring a certain harmonised level of procedural measures on computer data. These include: expedited preservation of stored computer data (Art. 16), production order (Art. 18), search and seizure of stored computer data (Art. 19), real-time collection of traffic data (Art. 20), and interception of content data (Art. 21). Based on the national provisions, the handling EDPs may order or request the issuing of the order (if judicial authorisation is required) for expedited preservation and/or production of computer data and ask the technical support to facilitate access to this data.

2. Scenario 2: e-evidence located within the territorial jurisdiction of an EPPO Member State other than the one of the handling EDP

If e-evidence is located in the territory of a Member State other than the one of the handling EDP, the latter can make use of the provisions of Art. 31 EPPO Regulation. This article represents a self-standing, *sui generis* legal basis for cross-border investigations of the EPPO.[11] The handling EDP sends an order for preservation/production of data to an assisting EDP from the Member State in question, who will then implement the measure there. If judicial authorisation is required under the legislation of the Member State where the data is located, the assisting EDP must obtain prior authorisation for the execution of the order from the competent court of his/her Member State.

3. Scenario 3: e-evidence located within the territorial jurisdiction of non-participating Member States other than Denmark and Ireland

To date, five EU Member States are not yet members of the EPPO. Three of them, i.e., Hungary, Sweden, and Poland, are bound by and have transposed in their national legislation Directive 2014/41 regarding the European Investigation Order in criminal matters (EIO Directive).[12] The collection of computer data which is located in the territory of one of these three non-participating Member States by the EPPO is governed by the provisions of the EIO Directive. In turn, the EIO is defined as a judicial decision issued or validated by a judicial authority in any one EU country for the gathering of evidence in criminal matters carried out in another EU country. Thus, in practice, the handling EDP will need to issue an EIO for the preservation/production of e-evidence on the basis of the national legal framework transposing the EIO in his/her country and send it for execution to the competent authority of the non-participating Member State. In this scenario, the EIO provides the EPPO with a simpler and faster alternative to the traditional mutual legal assistance instruments for requesting evidence, which are subject to strict deadlines and limited possibilities for refusal by the executing state.

4. Scenario 4: e-evidence located within the territorial jurisdiction of a Party to the Budapest Convention on Cybercrime (including non-participating Member State Denmark)

The Council of Europe Convention on Cybercrime (Budapest Convention) is a comprehensive and coherent international agreement on cybercrime and electronic evidence in criminal matters. It includes provisions to be implemented at national level, for both substantive and procedural law, and sets the rules for international cooperation for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form. To date, 68 countries are Parties to the Budapest Convention, including all EU Member States (except Ireland).

The Budapest Convention has high practical relevance for the criminal justice authorities of the Parties as it does not only concern computer-related crime, but any type of crime that requires the preservation/production of e-evidence. International cooperation in criminal matters under the Budapest Convention is regulated in Chapter III. For the preservation and collection of e-evidence, Section 2 of this Chapter (Arts. 29 to 34) is relevant, governing mutual legal assistance regarding provisional and investigative measures. The provisions include the following:

- Expedited preservation of stored computer data (Art. 29);
- Expedited disclosure of preserved traffic data (Art. 30);
- Mutual assistance regarding accessing of stored computer data (Art. 31);
- Trans-border access to stored computer data with consent or publicly available (Art. 32);
- Mutual assistance regarding real-time collection of traffic data (Art. 33);
- Mutual assistance regarding the interception of content data (Art. 34).

The Parties to the Budapest Convention can also make use of a 24/7 Network of contact points established under Art. 35. This network can facilitate the execution of preservation requests and production orders as well as provide assistance with regard to legal and technical information or locating suspects.

If data is located in a territory under the jurisdiction of a Party to the Budapest Convention, a criminal justice authority from another Party can apply the provisions of the Budapest Convention and request the preservation/collection of data directly, via the 24/7 Network, or via the authorities competent for international cooperation. While the EPPO is not a Party to the Budapest Convention and cannot make direct use of it, the handling EDP can make recourse to his/her powers as national prosecutor and request the data in accordance with the provisions of the Budapest Convention, under the conditions and limits set by Art. 104(5) EPPO Regulation. Accordingly, the handling EDP needs to "inform and where appropriate shall endeavour to obtain consent from the authorities of third countries that the evidence collected on that basis will be used by the EPPO for the purposes of [the EPPO] Regulation. In any case, the third country shall be duly informed that the final recipient of the reply to the request is the EPPO."

The handling EDP can also request the support of his/her country's 24/7 contact point or competent authority for sending and receiving mutual legal assistance (MLA) requests.[13] This can facilitate the process, as both the competent MLA authority and the 24/7 contact point have experience in working with the Budapest Convention and have established trustworthy relations with their counterparts from the other Parties to the Convention. In this context, Art. 28(1) EPPO Regulation enables the handling EDP "either to undertake the investigation measures and other measures on his/her own or instruct the competent authorities in his/

her Member State." In a broad interpretation of this provision, the handling EDP can issue a preservation/production order and instruct the national 24/7 contact point or the competent national MLA authority to send the request to the competent foreign contact point/MLA authority of the third country.

However, the chances of success of requests made either on the basis of Art. 104(5) or Art. 28(1) EPPO Regulation will depend on the openness and willingness to cooperate on the part of the third country's national contact point/MLA authority or other competent authorities. For the future, concluding working arrangements with these third countries based on Art. 99(3) EPPO Regulation could be a feasible option to improve cooperation.

5. Scenario 5: e-evidence located or stored in the territory of Ireland

Ireland neither participates in the EPPO nor is it a Party to the Budapest Convention on Cybercrime; nor is it bound by the EIO Directive (see above). Nevertheless, given that a number of major US Internet and social media providers are headquartered in Ireland, there is an important need to cooperate with the Irish authorities for securing and collecting e-evidence. Currently, the only possible option for any national criminal justice authority in the EU to collect e-evidence from the Irish jurisdiction is the use of traditional methods of international cooperation, i.e. using the MLA channels of the two applicable EU and CoE mechanisms: (1) Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union[14] and its Protocol, and (2) the European Convention on Mutual Assistance in Criminal Matters[15] and its two additional Protocols.

Despite the fact that all Member States participating in the EPPO have notified it as a competent authority for the application of the 2000 EU MLA Convention, Ireland has refused in practice to recognise these notifications and has been consistently rejecting the EPPO's requests for judicial cooperation.[16]

However, there is hope for the future. Ireland has a flexible opt-out option from EU legislation applicable in the area of freedom, security, and justice that allows the country to opt in or out of legislative initiatives on a case-by-case basis. As a result, Ireland has notified its wish to take part in the adoption and application of the EU's recent e-Evidence Regulation (Regulation (EU) 2023/1543)[17] due to enter into force in 2026. After the entry into force of this Regulation, EU criminal justice authorities will be able to issue and send preservation and production orders directly to service providers established in Ireland, with the latter having the obligation to provide the requested data under the conditions stipulated by the new EU legal framework on e-evidence.

6. Scenario 6: e-evidence located in the territory of a third country not covered by scenarios 1 to 5

For the collection of e-evidence from any jurisdiction not covered by the previous five scenarios, the EPPO needs to make use of the traditional channels of international cooperation in criminal matters, applicable to the collection of "classic" evidence. Cooperation with these jurisdictions can be based on two different scenarios: First, the EU is party to an international instrument on judicial cooperation and has declared the EPPO's competence for that particular instrument. Second, a Member State participating in the EPPO is party to an international agreement in criminal matters and it has notified EPPO as the competent authority for that specific instrument.

The EU has acceded to the UN Conventions against Transnational Organized Crime (UNTOC) and against Corruption (UNCAC). Accordingly, it has updated its declarations of competence for these UN Conventions and notified the EPPO as competent authority. However, the notification of the EPPO as competent authority for the purpose of these multilateral conventions is subject to the acceptance of the other Parties. All Member States participating in the EPPO have notified the CoE of the update to the list of competent authorities for the purpose of the 1959 MLA Convention and its additional Protocols and included the EPPO.

UNTOC, UNCAC, and the 1959 CoE MLA Convention are complemented by other bilateral or multilateral agreements on international cooperation in criminal matters signed by the Member States participating in the EPPO. Also here, the respective Member States participating in the EPPO must notify the EPPO as competent authority to their counterparts.

As regards cooperation with the United Kingdom, the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community and the United Kingdom of Great Britain and Northern Ireland (TCA) is applicable.[18] The EU has already notified the EPPO as competent authority for the application of the relevant MLA provisions of the TCA.

Similar to the cooperation with the Parties to the Budapest Convention, the handling EDP can also require e-evidence from other third countries by making use of the provisions of Art. 104(5) or Art. 28(1) EPPO Regulation. Likewise, the result of such requests will depend on the openness and willingness to cooperate on the part of the third country's competent authorities (see above).

7. Scenario 7: cooperation with US-based Internet and media service providers – voluntary disclosure

Relevant computer data is often stored and controlled by Internet and media service providers based in the United States (US ISPs), with the servers located in the US. The collection of this data through traditional MLA instruments, including the 2003 MLA Agreement between the EU and the USA[19], can be time-consuming and inefficient, with response times varying from six months to two years.[20] The EPPO has not yet been notified as competent authority for said MLA Agreement but has signed a memorandum of understanding and working arrangement with the US Department of Justice (DOJ) and the Department of Homeland Security (DHS),[21] in which the US side emphasised its intention to cooperate with the EPPO in the collection of evidence in EPPO cases "consistent with applicable legal frameworks."[22] The DOJ has asserted that it will "provide mutual legal assistance in response to a request made on behalf of a European Delegated Prosecutor handling the matter and transmitted between the appropriate authority of the EU Member State in which the investigation or prosecution is being carried out and the U.S. Central Authority for mutual legal assistance."[23]

However, several major US ISPs disclose data to foreign authorities on a voluntary basis – an approach which is also backed by US legislation. This is a pragmatic and lawful option to overcome some of the difficulties in swiftly obtaining e-evidence from the US. Google, Meta, Amazon, Apple, X, and others regularly disclose subscriber information or traffic data, and in some very limited cases, content data, to foreign criminal justice authorities, without requiring an MLA request sent via the competent US authorities. They also accept preservation requests directly sent to them by foreign authorities and have established dedicated teams to handle law enforcement and judicial requests for data. Transparency reports issued by said providers show that computer data is shared with foreign authorities in a significant number of cases.[24]

Voluntary disclosure of data by the US ISPs is problematic for the lack of predictability of the procedure and the discretionary power in the hands of the providers. Nevertheless, voluntary disclosure remains an option that can bring results and can facilitate the start and continuation of an investigation, at least until 2026 when the new EU e-evidence legislation will bring about important modifications.

https://doi.org/10.30709/eucrim-2023-016

A useful tool for contacting the specific US ISPs and for requesting the preservation of computer data, subscriber information, and traffic data is the "Practical Guide for Requesting Electronic Evidence Across Borders"[25] developed by UNODC jointly with several other international organisations and EU agencies. This guide is regularly updated and provides relevant practical information on the procedure, rules, and paths to be used by criminal justice authorities. While it is restricted to criminal justice practitioners, it can be accessed by practitioners working in the EU via the Europol Platform for Experts (EPE) and by all other criminal justice practitioners on the UNODC SHERLOC platform.

III. Data Protection Issues

The processing of operational personal data by the EPPO is governed by Arts 47 to 89 EPPO Regulation. Whenever the EPPO seeks to obtain electronic evidence from a competent authority or a private entity of a third country, including the non-EU parties to the Budapest Convention, it will, in most cases, provide some operational personal data to that authority/private party. For example, in order to request data preservation for a Gmail account, some operational personal data with regard to that email account needs to be disclosed. In addition, most of the third countries' authorities and private parties will request information on the crime, suspects, place, date etc. in order to reply to EPPO's request for data. For all these situations, the provisions of Art. 80 EPPO Regulation regarding the general principles for transfers of operational personal data by the EPPO are applicable. Similar to other EU legislation on the protection of personal data in criminal matters and international cooperation in criminal matters (e.g., the Law Enforcement Data Protection Directive[26], the Europol Regulation[27], and the Eurojust Regulation[28]), the EPPO Regulation provides for a limited number of cases in which the EPPO is allowed to transfer operational personal data to authorities or private parties outside the EU.

A transfer pursuant to Art. 81 EPPO Regulation is currently not an option for the EPPO as no adequacy decision has been issued by the European Commission on the basis of Art. 36 Directive (EU) 2016/680. As far as cooperation with the United Kingdom is concerned, the EPPO can rely on Art. 82(1) lit. a) EPPO Regulation because the TCA (as a legally binding instrument) includes appropriate safeguards with regard to the protection of operational personal data. In other cases, the EPPO can make recourse to the provisions of Art. 82(1) lit. b) or Art. 83 EPPO Regulation. According to Art. 82(1) lit. b) EPPO Regulation, transfers to third countries are possible when the EPPO has assessed all the circumstances surrounding the transfer of operational personal data and concluded that appropriate safeguards are in place with regard to the protection of personal data in that third country. Art. 83 EPPO Regulation stipulates derogatory situations in which transfer is specifically possible.[29] In the case of a possible transfer of operational personal data both on the basis of Art. 82(1) lit b) and Art. 83 EPPO Regulation, and subsequent transfer of operational personal data, the handling EDP needs to carry out an assessment and fill in a report/note justifying the measure prior to sending a request for e-evidence. This report/note must be registered in EPPO's Case Management System (CMS).

The assessment made by the handling EDP on whether the third country has appropriate safeguards with regard to the protection of personal data may take into consideration, *inter alia*, the current working arrangements concluded by the EPPO on the basis of Art. 99 EPPO Regulation with authorities of the respective third country. While Art. 99(3) EPPO Regulation explicitly stipulates that the working arrangements "may neither form the basis for allowing the exchange of personal data nor have legally binding effects on the Union or its Member States," the EDP is free to consider the data protection provisions in the working arrangement as one (but not the only one) element supporting his/her assessment of the existence of appropriate safeguards.

https://doi.org/10.30709/eucrim-2023-016

In future, Art. 82(1) lit a) EPPO Regulation (transfers on the basis of appropriate safeguards in a legally binding instrument) will gain importance when the Second Additional Protocol to the Cybercrime Convention[30] and a modernised Council of Europe Data Protection Convention ("Convention 108+")[31] enter into force and are ratified by a number of third countries.

IV. Conclusion

Given the increasing number of EPPO investigations, in which computer data are required to prove the commission of a criminal offence and to identify the perpetrators and the crime proceeds, the EPPO has to apply the legal frameworks, rules, procedures, and networks at its disposal. Otherwise, the EPPO could not efficiently collect such computer data and transform them into evidence accepted at trial. The applicable instruments for EPPO's handling EDPs vary depending on where the data are located. As has been shown in this article, sometimes complementary instruments apply, and sometimes the competent EDP must find pragmatic ways to obtain the best results.

In most cases, cross-border requests for e-evidence involve the (initial) transfer of operational personal data by the EPPO to authorities or private parties outside the European Union. Thus, the protection of personal data must be taken into thorough consideration, and the EDP must undertake to justify the transfer of personal data to third countries in line with the data protection rules in the EPPO Regulation in several ways.

Legal developments at the EU and international levels will unlock further possibilities for the EPPO to collect e-evidence in future. However, respecting the individual rights of data subjects must remain paramount even under these new set-ups.

---

1. Cf. <https://www.eppo.europa.eu/en/mission-and-tasks>. All links in this article were last accessed on 29 September 2023.↩
2. Commission Staff Working Document, Impact Assessment - Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD(2018) 118 final, p. 14.↩
3. Cybercrime Convention Committee (T-CY), *Criminal justice access to data in the cloud: challenges - Discussion paper*, 26 May 2015, <https://rm.coe.int/1680304b59>.↩
4. Art. 8 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), *O.J.* L 283, 31.10.2017, 1. Hereinafter: EPPO Regulation.↩
5. Art. 2(5) EPPO Regulation: "'handling European Delegated Prosecutor' means a European Delegated Prosecutor responsible for the investigations and prosecutions, which he/she has initiated, which have been allocated to him/her or which he/she has taken over using the right of evocation according to Article 27."↩
6. Art.2(6) EPPO Regulation: - "'assisting European Delegated Prosecutor' means a European Delegated Prosecutor located in a Member State, other than the Member State of the handling European Delegated Prosecutor, where an investigation or other measure assigned to him/her is to be carried out."↩
7. As of September 2023, these are: Denmark. Hungary, Ireland, Poland, and Sweden.↩
8. CETS No. 185, available at: <https://rm.coe.int/1680081561>.↩
9. Cf. <https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en>.↩
10. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224>.↩
11. Section 1, Article 1 of the Decision of the College of the European Public Prosecutor's Office of 26 January 2022 adopting Guidelines on the Application Of Article 31 Of Regulation (EU) 2017 /1939, available at: <https://www.eppo.europa.eu/sites/default/files/2022-02/2022.006_Decision_adopting_Guidelines_on_the_application_of_article_31_of_the_EPPO_Regulation.pdf>.↩
12. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *O.J.* L 130, 1.5.2014, 1.↩
13. Art. 27 para. 2 lit.a) Budapest Convention on Cybercrime: Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their *transmission to the authorities competent for their execution* (emphasis by author).↩
14. *O.J.* C 197, 12.7.2000, 3.↩
15. CETS No. 030.↩
16. Cf. <https://www.eppo.europa.eu/en/news/european-chief-prosecutor-addresses-letter-commission-irelands-refusal-cooperate-eppo>.↩

17. Regulation (EU) 2023/1543) of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *O.J.* L 191, 28.7.2023, 118.↩
18. *O.J.* L 149, 30.4.2021, 10.↩
19. Agreement on mutual legal assistance between the European Union and the United States of America, *O.J.* L 181, 19.7.2003, 34.↩
20. T-CY assessment report: *The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, p. 123, available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>.↩
21. Memorandum of Understanding and Working Arrangement on Cooperation between the European Public Prosecutor's Office, on the one side, and the United States Department of Justice and Department of Homeland Security, on the other side, available at: <https://www.eppo.europa.eu/sites/default/files/2022-07/WA%20EPPO-US-signed-EPPO.pdf>.↩
22. Memorandum of Understanding and Working Arrangement, *op. cit*. (n. 21), Section 3.↩
23. *Idem* 13.↩
24. T-CY, *Criminal justice access to data in the cloud: Cooperation with "foreign" service providers* - Background paper, 3 May 2016, available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d>.↩
25. Cf. <https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html>.↩
26. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA., *O.J.* L 119, 4.5.2016, 89.↩
27. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA., *O.J.* L 283, 31.10.2017, 1.↩
28. Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA., *O.J.* L 295, 21.11.2018, 138.↩
29. (a) in order to protect the vital interests of the data subject or another person; (b) to safeguard legitimate interests of the data subject; (c) for the prevention of an immediate and serious threat to public security of a Member State of the European Union or a third country; or (d) in individual cases for the performance of the tasks of the EPPO, unless the EPPO determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer.↩
30. Cf. <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224>.↩
31. Cf. <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65c0>.↩

Author statement

The views expressed in this article are exclusively those of the author and cannot be attributed to the institution that employs him.

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of

legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union