The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice

An Introduction to the New EU Package on E-evidence

Adam Juszczak, Elisa Sason *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

Digital technologies have advanced more rapidly than any other innovation in modern history and they permeate our daily lives. The benefits to our societies and economies are numerous, but the risks of cyberattacks and crime have also increased. The EU is committed to protecting its citizens against these risks in the Area of Freedom, Security and Justice. Prevention, detection, and enforcement form key components of the EU's security architecture. Making use of the benefits of digital technologies and ensuring a high level of security across the Union were driving forces behind the latest building block in this architecture: the e-evidence package. Recently adopted, it aims to ensure that judicial and law enforcement authorities can obtain electronic evidence across the EU and beyond in a swift and legally sound manner for the purpose of investigations and prosecutions in criminal cases.

This article provides an introduction to the two new EU instruments: the Regulation on European Production/Preservation Orders and the Directive on the designation of designated establishments and the appointment of legal representatives. The authors outline the key elements of this new set of rules and illustrate their implications for stakeholders. Furthermore, the borderless and open character of digital technology also makes it imperative to analyse existing and potential new international agreements in this field, since they will have an impact on the effectiveness of the enacted EU e-evidence package.

The article concludes that the adoption of the EU e-evidence rules is an important step in the joint efforts to fight crime effectively. Fundamentally relying on the principle of mutual trust among the EU Member States and a presumption of their compliance with Union law, the rule of law, and fundamental rights and values, the application of the e-evidence package will nonetheless require constant scrutiny, monitoring, and cooperation between all actors involved.

AUTHORS

Adam Juszczak

European Commission

Elisa Sason

Policy Coordinator
European Commission

CITE THIS ARTICLE

Juszczak, A., & Sason, E. (2023). The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice : An Introduction to the New EU Package on E-evidence. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2023-014

Published in eucrim 2023, Vol. 18(2) pp 182 – 200

https://eucrim.eu

ISSN:

I. Introduction

While it is common knowledge that digitalisation brings numerous benefits to our societies and economies, criminals are massively (mis-)using digital technologies to plan and commit criminal offences. Ensuring a high level of cybersecurity for digital products and services and having in place adequate tools for law enforcement authorities to investigate and prosecute criminal offences are ultimately two sides of the same coin. Recent developments, such as the COVID-19 pandemic and Russia's war against Ukraine, reaffirm the need for the EU to protect its citizens against the exploitation of known and new vulnerabilities, in full respect of fundamental rights. Prevention, detection, and enforcement form key components of the EU's security architecture.[1]

In the aftermath of the 2016 terrorist attacks, the Council adopted conclusions on improving criminal justice in cyberspace.[2] In these conclusions, the Commission was requested *inter alia*

"to develop a common framework for cooperation with service providers for the purpose of obtaining specific categories of data, in particular subscriber data, when allowed by third countries legislation, or any other comparable solution that allows for a quick and lawful disclosure of such data" and "to find ways, in association with Member States and, where necessary, third countries, as a matter of priority, to secure and obtain e-evidence more quickly and effectively by streamlining the use of mutual legal assistance proceedings and, where applicable, mutual recognition."

Similarly, in its Resolution of 2017,[3] the European Parliament called on the Commission to put forward a European legal framework for e-evidence, noting that "a common European approach to criminal justice in cyberspace is a matter of priority, as it will improve the enforcement of the rule of law in cyberspace and facilitate the obtaining of e-evidence in criminal proceedings."

To ensure that judicial and law enforcement authorities can obtain electronic evidence across the EU and beyond in a swift and legally sound manner for the purpose of investigations and prosecutions in criminal cases, the Commission proposed on 17 April 2018 a legislative package[4] composed of a Regulation on European Production and Preservation Orders and a Directive on the appointment of legal representatives. According to the Commission, cross-border access to electronic evidence for criminal investigations is needed in 85% of investigations, with 65% of the total requests going to providers based in another jurisdiction.[5] The volatile nature of electronic evidence makes access by law enforcement authorities essential, particularly in view of presenting it as admissible evidence before courts. Compared to traditional mutual recognition instruments, the novelty of these proposals is that orders may be directly addressed to a representative of a service provider in another Member State, without the authority of that other Member State being systematically involved in the process.

Having an internal EU framework in place – ideally followed by its proper application in practice – is, however, not the end of the story. Ensuring coherence and consistency between the EU's e-evidence rules and international agreements already agreed or still under negotiation, such as the Second Additional Protocol to the Budapest Convention of the Council of Europe, the United Nations Cybercrime Convention, and the EU-U.S. e-evidence agreement, is pivotal for the legal certainty of all stakeholders affected by this newly adopted framework.

This article provides a short background on the negotiations concerning the e-evidence proposal package (section II), outlines the key elements of the enacted e-evidence package (section III), and illustrates the implications of the new set of rules for stakeholders (section IV). It also touches upon existing links with international agreements (section V) and ends with a number of concluding remarks (section VI).

https://doi.org/10.30709/eucrim-2023-014

II. Negotiations and Adoption of the E-evidence Package

Following the adoption of the Commission's proposal in 2018, it took five years for co-legislators to agree on this package. The proposal was welcomed and garnered support for having in place faster tools for obtaining electronic evidence, but it also faced criticism in the form of warnings not to lower existing standards, particularly as regards the protection of fundamental rights.[6]

It is telling that seven Member States, including Germany and the Netherlands,[7] could not support the General Approach adopted by the Council in December 2018.[8] In addition, the high number of amendments proposed by the European Parliament – the Parliament put forward 841 amendments[9] – demonstrates the difficult path towards finding a compromise. The most contentious points of the negotiations were: the design of the notification mechanism, namely whether the authority of the Member State in which the service provider or legal representative is located should be involved in reviewing the Order; if so, for which type(s) of data; and whether the authority may assert grounds to refuse requests.

After eight trilogues, political agreement was reached in November 2022 and confirmed in Council (Coreper) and the European Parliament (LIBE Committee) in January 2023. The Regulation and Directive were published in the Official Journal on 28 July 2023.[10] While the Regulation will come to application 36 months after its date of entry into force, i.e., on 18 August 2026,[11] Member States will have 30 months to transpose the Directive after its entry into force, i.e., on 18 February 2026.[12] This allows Member States to make the necessary adaptations in their national laws and put everything in place before the e-evidence package starts to apply.[13]

III. Key Elements of the Enacted E-evidence Package

With its new e-evidence package, the EU introduces an entirely new system of obtaining electronic evidence in criminal proceedings by directly addressing private providers of communication, data storage, and internet infrastructure services located in another Member State – without, in principle, the need to involve the national authorities of the Member State in which the service provider is located. Such an approach can only function properly on the basis of a high level of mutual trust between the Member States.[14]

The new EU package on e-evidence is built on two distinct pieces of legislation:

- Regulation (EU) 2023/1543 lays down the rules and safeguards for national authorities to order service providers located in another Member State to preserve and produce e-evidence for the purpose of carrying out criminal proceedings;
- Directive (EU) 2023/1544 sets out, by contrast, harmonised rules on the designation of designated establishments or legal representatives by the service providers in order to ensure receipt, compliance with, and enforcement of orders issued by the competent authorities in the Member States for the purpose of gathering electronic evidence under the Regulation.[15]

Both legal acts shall be described in the following subsections.

1. Regulation on E-evidence

The Regulation, which is based on Art. 82(1) of the Treaty on the Functioning of the European Union (TFEU), introduces two new central instruments applicable across the Union for the purpose of obtaining electronic

https://doi.org/10.30709/eucrim-2023-014

evidence in criminal proceedings – the European Production Order and the European Preservation Order. The choice of legal basis was subject to strong criticism but was not changed by the legislator.[16]

These instruments are defined as decisions issued or validated by the judicial authority of a Member State and addressed to a designated establishment or legal representative of a service provider offering services in the Union and located in another Member State for the purpose of producing electronic evidence or for preserving electronic evidence with a view of a subsequent request for production, respectively.[17] With the European Preservation Order, judicial authorities may prevent foreign service providers from deleting or altering data, while the European Production Order enables the authorities to request preserved information directly from the service providers immediately or at a later stage.

To this end, the Regulation governs the conditions for the issuing of these instruments, its execution by the service providers, notification of and grounds of refusal for the executing Member State, the enforcement and penalties procedure, rights of the persons whose data is sought, a review procedure in case there are conflicting obligations with laws of a third state, provisions on standardised certificates and a decentralised IT system, and lastly rules governing the costs.

The Regulation does not, however, provide for a complete and exhaustive set of rules governing the application of the European Production Order and the European Preservation Order but instead refers on numerous occasions to rules provided under national law.

a) Subject matter and scope of the Regulation (Articles 1 and 2)

The material scope of application of the Regulation is limited to orders in the context of and for the purpose of criminal proceedings and for the execution of custodial sentences or detention orders of at least four months imposed by a decision not rendered *in absentia*. The orders may also be issued in criminal proceedings directed against a legal person. This means that these instruments cannot be used for preventive purposes or as a means of continuous surveillance. It requires the existence of concrete criminal proceedings, meaning that there is neither room for these instruments before criminal proceedings have commenced, nor once they have been terminated. Moreover, the Regulation also clarifies that it does not apply in mutual legal assistance proceedings, for which other respective instruments are to be used.

The Regulation defines the term "electronic evidence" as subscriber data, traffic data or content data stored by or on behalf of a service provider, in an electronic form,[18] i.e., emails, text messages or content from messaging apps, audio-visual content, or information about a user's online account. These categories of data correspond with the EU *acquis*[19] and established jurisprudence of the Court of Justice of the EU, as well as with the types of data used in the Member States and with international instruments.[20]

In terms of personal and territorial scope, the Regulation focuses on service providers offering services in the Union. The Regulation thereby targets service providers that provide electronic communication[21] and other information services[22] that enable users to communicate with each other or that process or store data on behalf of the users, such as telecom or social media companies. This includes voice-over IP, instant messaging, and email but also marketplaces and other hosting services as well as online gaming and gambling platforms.[23] Providers of internet infrastructure services, such as domain name registries, proxy service providers, and internet protocol registers, are also covered and of particular relevance, as they hold data that could allow for the identification of an individual or entity user or the victim of a criminal activity.[24]

The determination of whether a service provider is offering services in the Union is based on an assessment of two cumulative requirements. The first requirement concerns the availability of the services in a Member State, while the second requirement demands that there be a substantial connection, based on specific factual criteria, to that Member State or those Member States of the Union.[25] Such a substantial connection

is considered to exist if the service provider has an establishment physically located in the Union. In the absence of an establishment, the substantial connection is also considered to exist if the service provider has a significant number of users in one or more Member States or if it targets its activities towards one or more Member States of the Union. Thereby, the Regulation provides a number of evaluation criteria by which to determine such a substantial connection. This may be, for instance, the use of the local language/local currency, the possibility of ordering goods or services, the availability of applications in the local app store, or advertising activities.[26] However, the mere fact of having an online presence accessible in the Union, such as a website or an email address, taken in isolation, cannot be considered sufficient to determine that a service provider is offering services in the Union within the meaning of the Regulation.[27]

b) Issuing authority and issuing conditions (Articles 4, 5, and 6)

The question of who is authorised to issue a European Production Order or a European Preservation Order depends on the choice of instrument and the category of data requested. The reason for this differentiation can be explained with the different scope of the respective measure and the differing intensity and impact on fundamental rights of the various data categories.

European Production Order

A European Production Order may be issued by a judicial authority[28] – in the reading of the Regulation this is a judge, a court, an investigating judge, or a public prosecutor – if it concerns subscriber data and certain types of traffic data, namely data requested for the sole purpose of identifying the user, such as IP addresses and access numbers. In specific cases, the European Production Order may be also issued by any other competent authority in the issuing state acting as an investigating authority authorised under national law to order the gathering of evidence in criminal proceedings. In such event, however, the Order needs to be validated by a judicial authority, as set out above, who must examine the conformity of the Order with the conditions under the Regulation, and, if applicable, national law.

When the Order concerns the more intrusive categories of data – traffic data[29] and content data –, the issuing authority may be only a judge, a court, or an investigating judge but not a public prosecutor. Similarly, as above, the issuing authority may, in specific cases, be any other competent authority under national law, provided that the Order is duly validated by a judge, court, or investigating judge in the issuing Member State.

The Regulation departs from this mechanism in validly established emergency cases.[30] In the event of an emergency case, the issuing authority may, as an exception, issue a European Production Order in respect of subscriber data and data requested to identify a user without prior validation by a judicial authority if the validation could not be obtained on time and if the issuing authority could issue such an order in similar domestic cases without prior validation. In such a case, the issuing authority needs to obtain an *ex-post* validation without undue delay, at the latest within 48 hours. If the *ex-post* validation is not granted, the Order shall be withdrawn and the data obtained deleted or its use restricted.

The conditions for issuing a European Production Order differ according to the category of data: For subscriber data and user identification data,[31] a European Production Order may be issued for all criminal offences and for the execution of a custodial sentence or a detention order of at least four months.

In respect of the more intrusive traffic and content data, a European Production Order can only be issued for criminal offences punishable in the issuing Member State by a custodial sentence of a maximum of at least three years. In addition, in respect of specific enumerated offences, a European Production Order may be also issued irrespective of the scale of the custodial sentence if the offences were committed by means of an information system. The list of enumerated offences includes fraud and counterfeiting of non-cash

means of payment,[32] sexual abuse and exploitation of children,[33] attacks on IT systems,[34] and terrorist offences[35]. A European Production Order may also be issued for the execution of a custodial sentence or detention order of at least four months imposed for said enumerated criminal offences.

In addition to the more formal requirements on the information to be provided in the Order, there are also important limitations to the issuing of the European Production Order. These limitations concern situations in which the data is stored or processed by a service provider as a service to a public authority. In this case, the Order may only be issued if the public authority is located in the issuing Member State. Similar limitations apply to data stored or processed for professionals protected by professional privileges. The Regulation envisages a consultation procedure between the issuing authority and another Member State, in which the requested traffic or content data could be protected under immunities and privileges granted under the law of that other Member State, which applies to the service provider.

Irrespective of the category of data, the issuing authority needs to conduct a necessity and proportionality test and take into account the rights of the suspect or accused person. Lastly and importantly, the European Production Order may be only issued if a similar order could have been issued under the same conditions in a similar domestic case.

European Preservation Order

By contrast, in the case of the European Preservation Order, a differentiation depending on the data categories does not exist. Accordingly, the European Preservation Order may be ordered for all categories of data by a judicial authority – judge, court, investigating judge, or public prosecutor – or, in a specific case, by any other competent authority in the issuing Member State that acts as an investigating authority and is authorised under national law to order the gathering of evidence in criminal proceedings, provided that the Order has been validated by a judicial authority. The special rule governing emergency cases applies here in the same way as it does for the European Production Order.

The European Preservation Order may be issued if the issuing authority considers the Order necessary and proportionate for the purpose of preventing the removal, deletion, or alteration of data in view of a subsequent request for production, not only via the European Production Order but also via mutual legal assistance or a European Investigation Order. The rights of the suspected or accused persons must be taken into account. The European Preservation Order may be issued in respect of all criminal offences, provided that it could have been ordered under the same conditions in a similar domestic case and for the execution of a custodial sentence or a detention order of at least four months.

The conditions for the issuing of a European Preservation Order envisage a mandatory set of information to be provided with the Order, similar to but less comprehensive than that for the European Production Order. The Regulation also provides for a limitation on data stored or processed for a public authority; however, there is no such limitation in respect of professionals protected either by a professional privilege or by other types of privileges. The latter aspect should, however, be duly considered during the obligatory necessity and proportionality check to be conducted by the issuing authority in the process of issuing the Order.[36]

c) Addressees of the Orders and addressees' obligations (Articles 7, 10, and 11)

Addressees of the European Production and Preservation Orders are the designated establishments or legal representatives of the service providers.[37] In emergency cases,[38] the Orders may be directed to any other establishment or legal representative of the service provider, if the designated establishment or legal representative do not react or have not yet been designated.[39]

As regards the obligations, the European Production Order constitutes a binding decision of an issuing authority of a Member State obliging a service provider to produce electronic evidence within 10 days, or eight hours in emergency cases. Notification of the enforcing Member State pursuant to Art. 8 of the Regulation develops a suspensive effect on these obligations, save for emergency cases.[40] However, the strict deadlines imposed upon the service providers do not, in effect, change if the enforcing Member State does not raise any grounds for refusal. This means that service providers may need to be prepared to preserve and produce the requested data within the set 10-day period. If the service provider transmitted data to the issuing authority, while the enforcing Member State subsequently raised a valid ground for refusal, such data must be deleted or otherwise restricted, or, in the event that the enforcing authority has specified conditions, the issuing authority must comply with these conditions when using the data.[41]

The Regulation provides for a consultation mechanism, but no grounds for refusal, in the event that the service provider raises legal, formal, or factual impediments when complying with its obligations to execute the European Production Order. Accordingly, if the service provider raises concerns that the European Production Order could interfere with immunities and privileges, or with rules on freedom of the press or freedom of expression in the enforcing Member State, it shall inform both the issuing and the enforcing Member State. In such a case, the issuing authority may decide on its own motion or on request by the enforcing authority to withdraw, adapt, or maintain the Order. The enforcing authority may also decide to invoke a ground for refusal, provided it has such a right under Art. 8 of the Regulation. A similar consultation mechanism also applies in situations in which the service provider cannot comply with the European Production Order because the Order is incomplete, contains manifest errors or insufficient information, or because it is *de facto* impossible to execute it.

Generally, whenever the service provider for any other reason does not provide the requested information or cannot meet the deadline, it shall inform the issuing authority as well as the enforcing authority referred to in the Order to settle the matter expeditiously. In any case, the service provider has to preserve the data until it is produced, unless the service provider is informed that the preservation is no longer necessary.

Likewise, the European Preservation Order also constitutes a binding decision on a service provider, with the difference being the aim to preserve electronic evidence, with a view to a subsequent request for production via mutual legal assistance, a European Investigation Order, or a European Production Order. To this end, the service provider is obliged to preserve the requested data for a period of 60 days, after which the preservation shall cease. However, if the issuing authority confirms that a European Production Order has been already issued, the service provider needs to preserve the data as long as necessary in order to be able to produce it. In the event that a European Production Order has not yet been issued, the issuing authority may extend the initial 60-day period to preserve the data for an additional 30 days, with the aim of issuing the Order. As in the case of the European Production Order, the Regulation envisages also a consultation mechanism in the event that the service provider raises legal, formal, or factual impediments to comply with its obligations to execute the European Preservation Order.

d) Notification and grounds of refusal of the enforcing Member State (Articles 8 and 12)

A point fervently discussed during the negotiations concerned the extent of the involvement of competent authorities in the enforcing Member State and, in particular, whether the enforcing Member State should have any grounds to refuse the execution of the Orders. While the initial Commission proposal did not envisage any role for the enforcing Member State other than to facilitate the enforcement of the Orders, Art. 8 of the Regulation now stipulates situations in which the enforcing Member States must be notified and Art. 12 grants that Member State specific grounds to refuse the enforcement of a European Production Order.

Thus, whenever a European Production Order is issued for the production of traffic[42] or content data, the issuing authority needs to notify the competent authority of the enforcing Member State and transmit the European Production Order Certificate[43] at the same time it is transmitted to the service provider. The issuing authority also needs to include any additional information that enables the enforcing authority to assess the possibility of raising a ground for refusal. The notification of the enforcing Member State has a suspensive effect[44] on the obligation of the service provider, unless the matter concerns an emergency case, as defined in Art. 3(18).

The Regulation defines however an important exception from the notification requirement: there is no need to notify, if there are reasonable grounds at the time of issuing the Order that the offence was, is being, or is likely to be committed in the issuing Member State and that the person whose data is sought resides in that Member State (residence criterion).[45] Cases that do not affect the enforcing Member State should not lead to a notification. Similarly, the nationality of the person whose data is sought does not play a role.[46] The assessment of whether or not this exclusion is applicable rests solely with the issuing authority and, in this way, the issuing authority determines whether the competent authority in the enforcing Member State is granted the possibility to raise grounds of refusal of the European Production Order.

The grounds for refusal granted to the enforcing Member State are limited to reasons related to the principle of *ne bis in idem,* privileges and immunities, freedom of press and freedom of expression, and fundamental rights – whereby this latter reason is particularly subject to various limiting caveats.[47] In addition, Member States may invoke a refusal ground if the conduct for which the Order was issued does not constitute an offence under the law of the enforcing Member State (double criminality). The double criminality ground cannot, however, be invoked in relation to specific listed categories of offences[48] that are punishable with a custodial sentence or a detention order for a maximum period of at least three years in the issuing Member State. The enforcing authority is required to raise its grounds for refusal[49] within a period of ten days, or 96 hours (four days) in emergency cases, failing which it is deemed that the grounds for refusal have not been raised.[50] The ensuing effect of raising the grounds for refusal is that the service providers must halt the execution of the Order and refrain from transferring the data to the issuing authority, while the latter is requested to withdraw the Order. The Regulation also envisages a consultation mechanism between the enforcing and issuing authorities prior taking the decision on raising the grounds for refusal. This allows the competent authorities to find appropriate ways to overcome any potential grounds for refusal by adapting the Order or withdrawing it entirely.

e) Enforcement and penalties procedure (Articles 15 and 16)

The Regulation establishes an enforcement procedure and a penalties regime in the event that the service provider fails to comply with the duty to execute a European Production or Preservation Order Certificate (hereinafter: "EPOC" and "EPOC-PR").[51] The same applies if the service provider fails to comply with the duty to set up state-of-the-art operational and technical measures to ensure confidentiality, secrecy, and integrity of the transmission of the documents and data produced or preserved, as envisaged in Art. 13(4). In so doing, the Regulation obliges the Member States to lay down the rules and measures for such pecuniary penalties and to notify the Commission thereof without delay.

The Regulation stipulates only that the penalties regime has to provide for effective, proportionate, and dissuasive pecuniary penalties; it generally leaves the possibility for sanctioning, including by means of criminal law, to national law. Still, the Regulation clarifies that the pecuniary penalty may amount to up to 2% of the total annual worldwide turnover of the service provider. Only if a service provider acts in good faith when complying with the requirements of the EPOC and EPOC-PR, it shall not be held liable for the prejudices to their users or third parties – without prejudice to the applicable data protection obligations.

https://doi.org/10.30709/eucrim-2023-014

In case of non-compliance with the duties under the Regulation, the issuing authority may request the competent authority in the enforcing Member State, i.e., the State in which the designated establishment has been established or in which the legal representative resides, to enforce the Order. To this end, the issuing authority needs to send to the enforcing authority the Order accompanied by the form in which the service provider outlines the reasons for the non-execution of the EPOC or EPOC-PR (Annex III to the Regulation) as well as any other relevant documents. Based on this information, the enforcing authority is obliged to recognise the Order as it is and take the necessary measures for its enforcement without undue delay, no later than five working days after receipt of the Order. To that end, the enforcing authority formally addresses the service provider and requests that it complies with the obligations by a set deadline. The enforcing authority also needs to inform the service provider about the penalties in case of non-compliance and about the possibility to oppose the execution for specific reasons,[52] as outlined in Art. 16(4) and Art. 16(5) of the Regulation.

In addition, the enforcing authority may itself deny the enforcement if it considers any of the grounds for denial stipulated in Art. 16(4) and Art. 16(5) to apply to the matter brought before it. These grounds for denial include those for formal and material reasons, such as incorrect issuing or validation of the Order, *de facto* impossibility to execute the Order, service that is out of scope of the Regulation, or a manifest breach of fundamental rights.

On the basis of the information available or additionally provided, the enforcing authority shall decide whether or not to enforce the Order or deny its recognition and notify the issuing authority and the service provider accordingly. In case of non-recognition, the Regulation envisages a consultation procedure with the issuing authority similar to the one for grounds for refusal. In case of enforcement, the enforcing authority is to obtain the data from the service provider and, in the event of non-compliance, impose pecuniary penalties in accordance with the penalties system provided under Art. 15. The penalty is subject to an effective judicial remedy and the service provider may take action against it.

f) Review procedure in case of conflicting obligations (Article 17)

The issuing of a European Production Order must comply with the conditions laid out in the Regulation and, to the extent required, national law as well as with fundamental principles.[53] It may be the case, however, that the European Production Order is in conflict with the laws of a third state, which prevents the service provider receiving the Order from executing it. This is particularly the case when large service providers are involved that operate in several jurisdictions and that are bound not only by EU law but also by their domestic laws.

In such situation, Art. 17 envisages that the service provider informs the issuing and enforcing authority and provides a reasoned objection within a period of ten days, which includes details on the law of the third state applicable to the case as well as the nature of the conflicting obligation. The mere circumstance that similar provisions governing the issuing of a production order for the purpose of gathering electronic evidence do not exist in the third state or the fact that data is stored there do not suffice.

Upon provision of the reasoned objection, the issuing authority must review the Order it had submitted against the reasons provided in the reasoned objection. If the issuing authority intends to uphold the Order, it needs to refer the matter to the competent court in its Member State. The execution of the Order is suspended pending the review procedure.

In the judicial proceedings, the competent court has to make an assessment as to whether the law of the third country applies in the case at hand at all and, if so, whether it prohibits disclosure of the data concerned. Should the court conclude that the law of the third state constitutes such prohibition, the court needs to strike a balance between the conflicting interests based on criteria set in the Regulation. These

criteria concern the underlying interests behind the prohibition, including the protection of fundamental rights and national security of the third state, the degree of connection with the respective jurisdictions, the degree of connection of the service provider and the third country, the interest in pursuing the investigations, and the consequences for the addressee and/or service provider, if it/they were to comply with the Regulation in violation of the laws of the third state.

To facilitate the assessment to be carried out by the court, the Regulation envisages that the court may seek information from the third state, without prejudice to the investigations. The court is even obliged to contact the third country authorities in the event the matter concerns fundamental rights or fundamental interests of state security of the third state.

Upon reaching its decision, the court shall inform the issuing authority, the service provider, and the enforcement authority of its decision. Although the Regulation does not envisage any obligation to inform the authorities of the third state, it may be assumed that information about the outcome of the proceedings will also be provided to those authorities, at least if there was relevant contact in the course of the review proceedings.

Needless to say, this matter and this procedure, whereby the court takes into account the law and interests of a third state, touch upon a complex and politically sensitive area. Given that many large service providers are located outside the Union, most notably in the USA, the conflicting obligations described above are likely to occur frequently. In order to avoid clashes with foreign jurisdictions, the EU should seek to establish greater certainty in respect of affected foreign jurisdictions as a matter of urgency (see to this effect below under V.1).

g) Rights of the person whose data is sought (Articles 13 and 18)

The Regulation already states in Art. 1(3) that fundamental rights and legal principles enshrined in the Charter and in Art. 6 of the Treaty on European Union will be fully safeguarded. Moreover, the entire set of EU directives for procedural rights in criminal proceedings[54] will also apply.

The person whose data is sought will, however, generally not be in a position to find out whether his/her data was subject to the measures under the Regulation. Art. 13(1) hence requires that the issuing authority inform that person without undue delay. When informing the person, the issuing authority has to include information about available remedies pursuant to Art. 18 of the Regulation. The issuing authority may, however, delay, restrict or omit informing the person whose data is sought to the extent and under the conditions of Directive 2016/680[55], primarily in order not to prejudice the criminal investigations. In such case, the issuing authority needs to indicate the reasons in the case file and provide a short justification in the Certificate.[56]

In this context, Art. 18 provides for effective remedies against measures imposed under the Regulation. This provision enables the person whose data was sought to challenge the legality of a measure, including its necessity and proportionality, before the competent court in the issuing Member State, no matter if the person concerned resides elsewhere. This right is without prejudice to the guarantees of fundamental rights also in the enforcing State.[57] If that person is a suspect or accused, he/she may make use of all the rights granted to it during the criminal proceedings for which the data was ordered.

Additional remedies may also follow from the General Data Protection Regulation[58] and Directive 2016/680, as well as legal remedies available under national law, whereby the same time limits and conditions for seeking a remedy in similar domestic cases apply. This aims to guarantee an effective exercise of the remedies for the persons concerned.[59]

Art. 18 makes an explicit reference only to the European Production Order, and it is unclear whether and if so to which extent effective remedies against a European Preservation Order are available.

Although the Regulation puts an explicit obligation on the issuing Member State and any other Member State, to which electronic evidence was transmitted, to ensure that the rights of defence and fairness of the proceedings are respected when assessing the evidence obtained, the approach taken on the availability of effective remedies is therefore somehow unsatisfactory.

h) Standardised and IT-driven procedure – certificates and decentralised IT system (Article 9, Chapter V and Annexes)

The Regulation also formalises the procedure by establishing a decentralised IT system and by annexing standard forms to be used when applying this new mechanism.

The decentralised IT system aims to ensure a swift, direct, and secure cross-border electronic exchange of case-related forms, data, and information. It will be comprised of the IT systems of Member States and of the Union's agencies and bodies in addition to interoperable access points through which they are connected. The designated establishments or legal representatives designated by the service providers will be able to access the national IT systems forming part of the decentralised IT system. Art. 22 of the Regulation entrusts the Commission with the creation, maintenance, and development of a reference implementation software, which Member States may apply instead of a national IT system. This measure, too, strives towards the greatest possible coherence in the practical application of the e-evidence rules.

Although communication and exchange, as a rule, are to take place via the decentralised IT system, there might be cases in which this is not possible, e.g. due to the disruption of the system, the nature of the transmitted material, technical limitations, legal constraints related to the admissibility of evidence, or exceptional circumstances.[60] In such a case, the Regulation states that the transmission shall be carried out via the most appropriate alternative means, taking into account the need for swiftness, security, and reliability of the exchange of information. Any transmission by alternative means shall be recorded in the decentralised IT system without undue delay.

The use of electronic communication means for the transmission of documents is flanked by Arts. 20 and 21, which state that such documents should be granted legal effect and be considered admissible in the context of cross-border judicial procedures under the Regulation. A qualified electronic seal or qualified electronic signature, as defined in Regulation (EU) No 910/2014,[61] is to be used.

In addition, the desired swift, direct, and secure cross-border communication and exchange is facilitated by providing a set of standardised documents, annexed to the Regulation, including the EPOC and the EPOC-PR, through which the Preservation and the Production Orders have to be transmitted. The certificates contain information relevant for the execution of the Orders, such as details on the issuing authority, the user, the requested data category and time range, the applicable law, reasons given in case of emergency, the grounds for the necessity and proportionality of the measure, and, in the case of the EPOC, the summary description of the case.[62] The certificates will be available in all official languages of the Union, and Member States may decide, at any time, that they will accept translations of EPOCs and EPOC-PRs, not only in their own official language but in one or more official language(s).[63]

i) Costs (Articles 14 and 23)

In view of the central role given to the service providers when gathering evidence for the purpose of criminal proceedings, the Regulation envisages in Art. 14 a reimbursement scheme, based on which the service providers may claim reimbursement of their costs from the issuing Member State. Reimbursement is only

granted, however, if this possibility is provided for in the national law of the issuing Member State for domestic orders in similar cases. Hence, whether and, if so, to what extent such reimbursement will be granted in practice will depend on the situation in the issuing Member State. The national practice often ranges from full reimbursement to full bearing of the costs.[64]

Another type of cost concerns costs related to the decentralised IT system. The decentralised IT system is essential for the written communication and data exchange between the competent authorities and the service providers as well as among the competent authorities themselves. Ensuring confidentiality, secrecy, and integrity of the transmissions of the documents and the data produced or preserved requires, in particular, that the service providers install state-of-the-art operational and technical measures, which, if not in place, may be sanctioned under Art. 15 of the Regulation. With regard to costs, Art. 23 envisages that each Member State, Union agency or body, and each service provider bears all costs related to the use and maintenance of or the interaction with the decentralised IT system, as the case may be.

2. Directive on the designation of establishments and appointment of legal representatives

While the Regulation regulates the rules under which the authority of a Member State may order a service provider offering services in the Union to produce or preserve electronic evidence for the purpose of criminal proceedings, the accompanying Directive lays down the rules and obligations ensuring that the orders and decisions issued under the Regulation reach the right addressees: the private service providers.[65] The aim of this legal act is to guarantee a coherent approach to imposing obligations on service providers – and Member States – in the context of gathering electronic evidence in criminal proceedings. The approach seeks to overcome the problems that previously resulted from the existence of different national rules and obligations and the fact that many service providers, though operating in the Union, are located outside the bloc.

By setting out the rules on the designation of establishments and the appointment of the service providers' legal representatives, the Directive establishes a clear channel of communication, and thus the necessary legal certainty, not only for the service providers, who were often uncertain whether they were obliged or allowed to follow up on a request in the past, but also for the competent national authorities across the Union, who may now quickly and efficiently direct their requests to the correct addressee.

This central element of the Directive – the designation of establishments and appointment of legal representatives by service providers – is flanked by the obligation for the Member States to set up a penalties regime to deal with any violation of the obligations under the Directive. They are also required to designate central authorities mandated to ensure a consistent and proportionate application of the Directive.

Although the Directive clearly pursues the purpose of facilitating the work of national authorities in gathering electronic evidence in criminal proceedings, it is based on Arts. 53 and 62 TFEU, which guarantee the freedom to provide services. This is explained somewhat briefly in the Explanatory Memorandum of the Commission Proposal where it is stated that the obligations following from the Directive would help eliminate obstacles to the freedom to provide services.[66] This choice of legal basis was subject to criticism during the negotiations, but, as it was the case with the Regulation, was not changed by the legislator.

a) The designation of designated establishments and legal representatives by the service providers (Articles 3 and 4)

The Directive states that Member States need to ensure that service providers offering services in the Union designate at least one addressee for the receipt of, compliance with, and enforcement of decisions and

orders issued by the competent authorities of Member States for the purpose of gathering evidence in criminal proceedings. To this end, the Directive targets the same service providers as those covered under the Regulation.[67]

Service providers that are established in the Union[68] and provide services in more than just one Member State[69] are requested to designate one or more designated establishments to be responsible for carrying out the functions described in the Directive. Service providers that are not established but offer their services in the Union (this applies to many large companies located in the USA) are required to appoint one or more legal representatives to be responsible for carrying out the functions described in the Directive. Thereby, the term "offer services in the Union" has the same meaning as that provided under the Regulation.[70] In the event that a service provider is established in a Member State that does not take part in the e-evidence package the service provider needs to appoint a legal representative in a Member State that does take part in this instruments.

The service providers are, in principle, free to choose how many designated establishments or, as applicable, legal representatives they designate or appoint and in which Member State(s). Member States cannot restrict this free choice.[71] For the purpose of operationality, however, the Directive states that the designated establishment should be established in a Member State in which the service provider provides its services or is established, and it should designate a designated establishment in one of the Member States taking part in a legal instrument referred to in the Directive (see below).[72] The same applies to the legal representative.[73] To ensure clarity, service providers must indicate the precise territorial scope of the designation, in the event that they designate several designated establishments or appoint several legal representatives, respectively.[74]

The Directive also allows for a designated establishment or legal representative to be shared by several service providers, unless this would impinge on data protection safeguards. This possibility for sharing may be particularly beneficial to small-sized and medium-sized enterprises.[75]

Although established by the Directive as part of the e-evidence package, the role of designated establishments and legal representatives is, pursuant to Art. 1(2), not confined to decisions and orders under the Regulation alone but may also apply in the context of the European Investigation Order[76] and the EU Convention on Mutual Legal Assistance.[77] Moreover, this concept may equally apply to decisions and orders for the purpose of gathering electronic evidence on the basis of national law.[78] However, this means that the procedures set out in the instruments mentioned come to application. It is then to ask whether these instruments permit the direct serving of orders in cross-border situations to the designated establishment or legal representative or whether they demand cooperation between competent judicial authorities.[79]

Accordingly, the service providers must take all measures to ensure that the designees/appointees are equipped with the necessary powers and resources to comply with the decisions and orders received from the authorities of any Member State participating in the instruments mentioned above. Member States are under a duty to verify whether this is and will remain the case (see also central authority below).

In terms of procedure, each service provider must notify the central authority in writing (see below) within a period of six months from the transposition deadline of the Directive or from the moment it starts offering services in the Union[80] about the Member State in which it is established or offers its services and where its designated establishment is established or where its legal representative resides, respectively. The notification should also provide information about the languages to be used[81] and the precise territorial scope of its designation.[82]

b) Penalties regime (Article 5)

Art. 5 of the Directive envisages a separate penalties regime in case there is a violation of the obligations imposed upon the service providers under the Directive. The Directive thereby clarifies that non-compliance cannot be justified on the grounds of, *e.g.,* inefficient internal procedures or lack of resources, insufficient powers, or the failure to notify a designated establishment or a legal representative. In case of non-compliance, the designated establishment or the legal representative and the service provider itself may be held jointly and severally liable, *i.e.,* each of them – the designated establishment or the legal representative and the service provider – may be sanctioned for non-compliance by any of them.[83]

The penalties to be imposed shall be effective, proportionate, and dissuasive. When determining the appropriate penalty, all relevant circumstances should be considered: the financial capacity of the service provider; the nature, gravity, and duration of the breach; whether it was committed intentionally or through negligence; and whether the service provider has been held responsible for similar previous breaches. Under no circumstances, however, should the sanctions envisage a permanent or temporary ban of the provision of services, [84] as it would run counter the very purpose of the Directive, the aim of which is to remove obstacles to the free provision of services in the Single Market.

Legal action following civil or administrative proceedings, including proceedings that can lead to sanctions, may, in principle, be applied in parallel to any sanctions under the Directive. In this context, the Directive also envisages a number of notification requirements for the Member States. Upon transposition of the Directive, Member States are obliged to notify the Commission of their rules and of measures enacted with regard to the sanctions regime; they must also provide updates should the rules be amended in the future. In addition, Member States have to inform the Commission annually about cases of non-compliance by service providers, the relevant enforcement action taken against them, and the sanctions imposed. These notification requirements should ensure the necessary transparency but also demonstrate the effectiveness of the measures.

c) Central authority (Article 6)

Member States are required to designate one or more central authorities to ensure a consistent application of the Directive and to ensure a seamless cooperation amongst the central authorities in other Member States, in particular by exchanging information and providing mutual assistance. This relates, in particular, to the enforcement actions as well as verifications of whether the designated establishments or legal representatives residing on their territory received from the service providers the necessary powers and resources. In this way it will be also apparent, whether the designated establishments or legal representatives cooperate with the competent authorities in accordance with the applicable legal framework.

To this end, the central authorities themselves are required to be equipped with sufficient powers to carry out the tasks entrusted to them, including coordination powers for enforcement actions between competent authorities in different Member States. For the coordination of an enforcement action, the central authorities may also involve the Commission if this could be relevant.[85] An additional aim of this coordination mechanism is to avoid positive or negative conflicts of competence amongst competent authorities in the Member States.

Furthermore, this new mechanism will also serve important transparency functions. The designation of the central authorities will make it easier for the service providers to provide notification about the designation and the contact details of their designated establishment or legal representative to the proper place in the Member State where their designated establishment is established or legal representative resides.

Accordingly, once Member States inform the Commission of their designated central authority or central authorities, the Commission will distribute a list of designated central authorities to all the Member States and make it also publicly available.

IV. Implications for Stakeholders

With the adoption of the e-evidence package, the time period for implementation and adaptation has started. Ensuring that the full e-evidence framework is properly and accurately implemented in the European and national legal orders requires the necessary time and effort on the part of all stakeholders involved. As shown in the previous sections, the complex nature of the adopted rules and procedures call for a careful analysis of the rights and obligations of all actors affected as well as of the reasonable expectations they may have from each other.

One of the main initial points of criticism regarding this initiative concerned the protection of fundamental rights, particularly in light of the proposed mechanism of direct cooperation between private entities and public authorities for the purpose of law enforcement activities.[86] While the role of service providers – that hold an unprecedented strong position in handling and keeping vast amount of information – in the European legal order has increased significantly over the past several years,[87] the area of criminal justice was not familiar yet with a direct role of private entities in the enforcement activities of national authorities across the Union. Service providers will in this way have to play multiple and even contradicting roles: serving as the extended arm of public law enforcement authorities, protecting the personal data of their customers, and ensuring their own legitimate business interests. It is not far-fetched to imagine that clients might wonder whether the service provider is sharing their personal data with law enforcement authorities and how they can find this out. The diverging interests might put the service providers in a difficult situation, and it remains to be seen how service providers will cope with this new role they have been given by the Union legislator with the e-evidence package and how they will strike a balance between the diverging interests. A procedure that remains largely confidential between the national authorities and the service provider, and hence undisclosed to the public, demands that greater attention be given to transparency and effective judicial review.

Whether this will be guaranteed in a satisfying manner remains to be seen. Just to give an obvious example: While the issuing authority should inform the person whose data is being sought about the data production without undue delay, the same issuing authority may decide, in accordance with national law, to delay, restrict, or even refrain from informing the person to the extent that/as long as the conditions of Directive 2016/680[88] are met. In practice, this means that the applicable rules vary per Member State and that the person whose data is being sought will not automatically know whether his/her data has been shared with law enforcement authorities, hence not be able to go against it. The person may not even find out that his/her data was sought in the first place if national law allows for omitting to inform the data subject for as long as "such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned". A mandatory (*ex post*) notification is not envisaged in the e-evidence package. If the person whose data is sought does become aware of the circumstance that his/her data was shared with national law enforcement and judicial authorities, the right to effective remedies against the European Production Order exist, including possible additional legal remedies in accordance with national law. For this specific situation, the rules stipulate that information should be provided in "due time" about the possibilities to seek remedies under national law and to ensure that they can be exercised effectively.

Although the involvement of judicial authorities in the enforcing Member State has increased with the adopted rules, particularly as regards the most sensitive data categories for which electronic evidence could

be requested, the necessary judicial control might quickly fall short of the needed effectiveness. Situations involving several Member States could soon overburden the judicial control mechanism envisaged under the Regulation, e.g., when data is requested by Member State A, from a service provider located in Member State B, with the person residing in (but not being a national of) Member State C, and providing professional services in Member State D. At the time of the request, it may neither be known to the authorities in Member State A (issuing Member State), nor the ones in Member State B (enforcing Member State) that the person whose data is being requested is carrying out journalistic activities in Member State D. In this scenario, Member State C (place of residence) and Member State D (place of professional activity) would not receive any notification of the request sent to Member State B by Member State A. This raises the question of an effective legal remedy, as the question in which Member State(s) the person concerned should or could seek legal remedies may not always be straightforward. Concerns about the final package have indeed been raised as regards media freedom and the possible misuse of confidential data belonging to journalists.[89] Similar concerns are also valid for persons subject to professional secrecy, such as defence lawyers or medical professionals.

From a law enforcement perspective, the new rules definitely provide a speedier framework for requesting data for law enforcement purposes compared to traditional mutual legal assistance instruments or even the European Investigation Order. Practice, however, will show whether service providers will actually be able to produce certain sets of data under the conditions imposed by the EU rules, particularly when there is no generalised obligation to retain data[90] and when orders to produce data only arrive at service providers after the commission of an offence and at the start of a criminal investigation, as required under the Regulation. By then, the data may have already been erased or can no longer be produced by the service provider.

Notwithstanding the foregoing, service providers will be required to make the necessary adaptations to their organisational structures – particularly by ensuring the necessary resources – at the risk of financial sanctions. Apart from that, they will be required to respond to requests for data on the basis of a mandatory and decentralised IT platform; the Commission will need to prepare implementing acts on this within two years after adoption of the Regulation.[91] Service providers should also be mindful of the possibility to claim reimbursement from the issuing State, in accordance with the national law of that State, of their costs for responding to a European Production Order or to a European Preservation Order if that possibility is provided for in the national law of the issuing State for domestic orders in similar situations (see above III.1 i)). As rules can vary, Member States are required to communicate to the Commission their national rules, which must also be made public. In view of the broad scope of EU rules and the high number of companies covered – telecommunication providers, cloud services, and over-the-top services –, these rules are expected to have a significant impact on the operationality of service providers.

V. International Dimension

The borderless and open character of modern technology has the effect that cybercrime is becoming increasingly transnational, involving offenders and victims located in multiple jurisdictions. To adapt to these circumstances, it is important that cross-border access to electronic evidence by competent authorities follows a consistent set of rules which can ideally stand the test of time. Various efforts to improve access to electronic evidence for the purpose of investigating and prosecuting cross-border cases have already been undertaken, and recent developments show a continuation of these efforts at the national, European, and international levels. Based on the principle of mutual trust, the enacted e-evidence package is intended to set the standard in gathering electronic evidence for the purpose of criminal proceedings in the European Union. It would be in the interest of the EU to strive for high standards, including standards on data protection, at the international level as well. This section provides a brief overview of the existing

international instruments that are relevant for the gathering of evidence in criminal proceedings. As will be seen, they also have an impact on the e-evidence package.

1. An EU-US E-evidence agreement

Finding a common approach between the EU and the USA that allows for cross-border access to data held by service providers in the EU or the USA has been an evergreen-priority on the justice and home affairs agenda. The United States of America are one of the main recipients, if not the main one, of mutual legal assistance (MLA) requests from EU Member States for access to electronic evidence, as the largest service providers are headquartered there. Given that the largest service providers are based in the USA and that the key instrument, namely mutual legal assistance between both continents, has its limits (notably its slowness),[92] this does not come out of blue. An EU-US e-evidence agreement could indeed help overcome current divergent approaches, which often rely on voluntary cooperation mechanisms between judicial authorities and service providers. Such an agreement could set common standards that also address conflicts of laws. Direct cooperation with service providers in the USA would be a significant improvement over the time-consuming classical mutual legal assistance process. Under the U.S. Stored Communications Act of 1986,[93] however, direct cooperation is limited to non-content data and the service providers are free to cooperate, while a disclosure of content data is prohibited. The United States CLOUD Act (Clarifying Lawful Overseas Use of Data), adopted on 23 March 2018, amends the Stored Communications Act of 1986 such that US service providers are obliged to comply with US orders to disclose content data and non-content data, regardless of where such data is stored, i.e., no matter whether the data is stored on servers located in the EU or not. The CLOUD Act allows the conclusion of executive agreements between the USA and foreign governments, on the basis of which US service providers would be able to deliver content data directly to the foreign governments. The scope of data covered by the CLOUD Act is stored data and the interception of wire or electronic communication with respect to serious crimes. The executive agreements are subject to a number of conditions, including that the domestic law of the third country and its implementation "affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection".[94] So far, the USA has concluded executive agreements under the CLOUD Act with the UK[95] and Australia[96] and has entered into negotiations with Canada.[97] The executive agreements concluded, however, all contain an important restriction prohibiting the transfer of data concerning US citizens and persons located in the USA.

The Council Decision authorising the opening of negotiations for an EU and US agreement on cross-border access to electronic evidence, together with its negotiating directives,[98] was adopted swiftly after being proposed by the Commission in February 2019. While the Council largely followed the Commission's approach, it is interesting to note that, compared to the proposal, the Council introduced two additional procedural rights safeguards to be reviewed in conjunction with the scope of the future agreement: (1) safeguards to ensure that data requested may be refused if the execution of the request is likely to be used in criminal proceedings that could lead to life imprisonment without the possibility of review and prospect of release; (2) specific safeguards for data protected by privileges and immunities and data whose disclosure would be contrary to the essential interests of a Member State.[99]

After the adoption of the EU's negotiation mandate in June 2019, negotiations were put on hold for a number of years. This was due to the fact that the negotiating directives set out not only that compatibility between the EU-US agreement and the EU rules of the e-evidence package be ensured but also that these rules serve as the baseline for the Union's negotiating position. This is why an agreement on the e-evidence package had to be reached first, before it was possible to enter into in-depth negotiations on the EU-US agreement. The negotiations resumed in March 2023[100] and are currently ongoing.

Time has not stood still, however, since the negotiations between the EU and US were halted in 2019. There have been a number of recent developments, including the fact that an agreement has been found on the Second Additional Protocol to the Budapest Convention (below 2.). The negotiating directives reflect in this respect that the future EU-US agreement should take precedence over the Budapest Convention as well as any agreement reached on the negotiations of the Second Additional Protocol, in so far as the provisions of the latter agreement cover issues dealt with by the EU-US agreement.[101] It is of relevance that the USA signed both the Budapest Convention and the Second Additional Protocol. Also noteworthy are the interconnection with the EU's data protection legislation and jurisprudence, including the General Data Protection Regulation (GDPR), and the recently adopted adequacy decision under the EU-U.S. Data Privacy Framework.[102] The same applies to the EU's approach towards digital sovereignty and cybersecurity.[103]

The conclusion of the executive agreement with the USA is essential for a seamless functioning of the e-evidence package. The agreement particularly has to clarify the binding nature of orders on service providers and also define the obligations for judicial authorities. It is hence indispensable that the negotiations with the USA on the executive agreement come to a timely conclusion, before the coming into application of the e-evidence package.

2. The Council of Europe Convention on Cybercrime ("Budapest Convention")

Following the adoption of the Budapest Convention in 2001, and its entry into force in 2004, 68 States have become official parties to the treaty to date.[104] According to its Explanatory Memorandum, the Convention aims to (1) harmonise the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime, (2) provide for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form, and (3) set up a fast and effective regime of international cooperation.[105] Despite its relative 'old' age, the Convention has not lost its relevance in modern practice, thanks to its technology-neutral language and high number of participating States.

Since its adoption 22 years ago, the Convention has been updated twice: The First Additional Protocol in 2002 extended the scope of the "mother Convention" by criminalising acts of a racist and xenophobic nature committed through computer networks. The Second Additional Protocol was adopted by the Committee of Ministers on 17 November 2021.

The Second Additional Protocol intends to step up the fight against cybercrime by strengthening the possibilities for judicial authorities to collect electronic evidence of a criminal offence for the purpose of specific criminal investigations or proceedings by means of additional tools, e.g., the possibility for two or more parties to establish a joint investigation team and the taking of testimonies and statements of witnesses or experts by video conference. In addition, the Second Additional Protocol provides rules on cooperation in emergency situations requiring an expedited response as well as rules on direct cooperation between competent authorities and service providers and entities in possession or control of pertinent information, including domain name registration information and subscriber data.

While the Convention applies only to the States that have ratified it and does not allow the EU to accede to it, the EU takes part in meetings of the Convention Committee as an observer and is committed to the Convention's promotion. The EU has played an essential role in ensuring that the Second Additional Protocol is coherent and consistent with Union law. Following up on the European Council Conclusions of October 2018,[106] the Commission adopted in February 2019 a Recommendation for a Council Decision with negotiating directives authorising the participation of the Commission, on behalf of the EU, in the negotiations on the

Second Additional Protocol.[107] At the JHA Council in June 2019, the Council gave its green light to the Commission to negotiate this instrument.[108] Compared to the Commission proposal for the negotiating directives, it should be noted that the Council added Art. 16 and Art. 82(1) TFEU as legal bases as well as specific rules on the procedure for negotiations.[109] The adoption of the Council Decision on 5 April 2022 ultimately authorised EU Member States to sign the Protocol.[110] The Protocol was opened for signature in May 2022 and has been signed by 37 States to date.[111] The Council Decision to authorise Member States to ratify the Protocol was adopted on in February 2023 in accordance with the procedure laid down in Art. 218(6) TFEU. The European Parliament gave its consent in January 2023, after it voted against referring the Protocol to the CJEU for an Opinion in November 2022.

The Second Additional Protocol will complement the EU rules on the e-evidence package. It has the benefit that, once fully ratified, it will apply globally to all 68 signatory countries of the Budapest Convention.

3. The United Nations Cybercrime Convention

The idea behind and push for having a UN Convention on Cooperation in Combating Cybercrime in place came from the Russian Federation in 2017.[112] Before the decision was taken to cease the Russian Federation's membership on the Council of Europe in response to its war against Ukraine,[113] the Russian Federation was the only member not party to the Budapest Convention; the Russian Federation held the view that the Convention encroaches upon its security and sovereignty.[114] In this light and coinciding in 2017 with the timing for launching negotiations on the Second Additional Protocol to the Budapest Convention, Russia's proposal for an international convention on cybercrime can only be regarded as an attempt to put in place a competing instrument. With 88 votes in favour to 58 against and 34 abstentions, the draft resolution of the Russian Federation was, nonetheless, adopted on 18 November 2019.[115]

Just one month later, the UN General Assembly adopted a resolution to establish an open-ended *ad hoc* intergovernmental committee of experts/representative of all regions to elaborate a comprehensive international convention on countering the use of information and communication technologies for criminal purposes (hereinafter: the UN Cybercrime Convention).[116] The agreement that a draft convention should be provided and the work schedule of the *ad hoc* committee were both endorsed by the General Assembly in May 2021.[117] If adopted, the Cybercrime Convention would be the first instrument at the UN level to combat cybercrime and would facilitate international judicial cooperation in criminal matters with third countries that are not party to the Budapest Convention and its Protocols. The proposed structure includes chapters on general provisions, criminal offences, procedural measures and law enforcement, international cooperation, technical assistance, preventive measures, mechanisms of implementation, and final provisions.[118]

With all EU Member States voting against the Resolution adopted by the UN General Assembly in 2019, the coordination of a uniform European position in the negotiations of the UN Cybercrime Convention is of crucial importance. In March 2022, the Commission issued a recommendation for a Council Decision with negotiating directives,[119] based on Art. 218(3) TFEU, allowing the Commission to negotiate the Convention on behalf of the EU. Two months later, the Council adopted its Decision,[120] adding Arts. 82(1) and (2) as well as Art. 83(1) TFEU as legal bases, taking into consideration that the new instrument may also affect EU rules on judicial cooperation in criminal matters. The Decision specifies in this regard that the Commission is to conduct negotiations on behalf of the EU for matters falling within its competence, in accordance with the Treaties and in respect of which the Union has adopted rules.[121] The guiding principles underpinning the EU's mandate refer most notably to establishing consistency with existing legislation, to guaranteeing a strong protection of human rights standards and fundamental freedoms, and to ensuring that definitions and procedures are sufficiently clear and specific.

With five negotiation sessions held so far, progress has already been made on the text of the draft Convention. The consolidated negotiating documents presented prior to the fourth and fifth sessions as well as the draft text of the Convention presented ahead of the sixth session[122] show how the Convention is taking shape, taking into account different proposals and statements, including those of the EU and its Member States.[123] The most recent consolidated negotiating document focused, amongst other things, on international cooperation and was published on the last day of the fifth session of the Ad Hoc Committee on 21 April 2023.[124] This document shows the sensitivities and complexities of the negotiations, including attention to the protection of personal data, extradition, and mutual legal assistance procedures. It also shows the committed approach of the EU and its Member States towards safeguarding fundamental rights and values. The plan is for the text of the future Convention to be finalised during a concluding session at the beginning of 2024 with a view for its adoption in September 2024. It remains to be seen whether the final text of the UN Convention will be consistent with and provide any added value to the existing international and EU legislative instruments, such as the Budapest Convention and its protocols.

VI. Conclusion

The adoption of the EU e-evidence rules is an important step forward towards facilitating effective cross-border cooperation in criminal matters, which, given the borderless dimension of criminal activity, is sure to become even more pressing over the next several years and decades. With the costs stemming from the (mis-)use of digital technologies for the purpose of committing crimes alone are expected to rise from 8.4 trillion US dollars in 2022 to 10.5 trillion US dollars by 2025,[125] it is clear that the fight against this growing phenomenon should be given a high priority at all levels. The newly adopted rules require all stakeholders – from judicial and law enforcement authorities to service providers and defence lawyers – to undertake all necessary efforts to ensure their timely and accurate implementation as well as their correct application in practice. The mechanism established under the e-evidence rules relies fundamentally on the principle of mutual trust among the EU Member States and a presumption of their compliance with Union law, the rule of law, and fundamental rights and values. It is of particular significance that five Member States issued statements upon adoption in which they express concerns regarding the protection of fundamental rights and the application of effective judicial review under the e-evidence package.[126] Hence, the application of the e-evidence package will require constant scrutiny, monitoring, and cooperation between all actors involved. Guaranteeing the necessary transparency and effective judicial review are key elements of this initiative. The practical application of these rules as well as ensuring coherence and consistency with initiatives at the international level – in particular the envisaged executive agreement between the EU and the USA – are, no doubt, essential components to effectively fight crimes in the European Area of Freedom, Security and Justice – today and in the future.

---

1. COM(2020) 605 final on the EU Security Union Strategy; COM(2021) 170 final on the EU Strategy to tackle Organised Crime; JOIN(2020) 18 final on the EU's Cybersecurity Strategy for the Digital Decade; COM(2020) 795 final on A Counter-Terrorism Agenda for the EU.↩
2. June 2016 Conclusions on improving criminal justice in cyberspace: <https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf>. All references to hyperlinks were last accessed on 16 October 2023.↩
3. European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)) - P8_TA(2017)0366.↩
4. Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final and proposal for a Directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final.↩
5. SWD(2018) 118 final on the Impact Assessment accompanying the e-evidence package.↩
6. See, for example, the statement of civil society organisations and bar associations of 4 March 2022: <https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2022/Coalition's%20remarks%20on%20EP%20package%20deal.pdf>.↩
7. <https://www.euractiv.com/section/digital/news/council-makes-half-hearted-agreement-on-e-evidence/>.↩
8. Council General Approach text of 12 December 2018: <https://data.consilium.europa.eu/doc/document/ST-15292-2018-INIT/en/pdf>.↩
9. European Parliament, Report - A9-0256/2020 of 11 December 2020: REPORT on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.↩

https://doi.org/10.30709/eucrim-2023-014

10. 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; Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, *O.J.* L 191, 28.7.2023, 181.↩
11. Art. 34(2) of the Regulation.↩
12. Art. 7(1) of the Directive.↩
13. In accordance with Protocol No 22 on the position of Denmark annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.↩
14. Cf. Recital 12 of the Regulation.↩
15. For the references of both acts in the Official Journal, see *op. cit.* (n. 10).↩
16. Cf. *e.g.,* M. Böse, An assessment of the Commission's proposals on electronic evidence, <http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf>; P. Topalnakos, "Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings", in this issue.↩
17. Art. 3(1) and (2) of the Regulation.↩
18. Art. 3(8) of the Regulation.↩
19. Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *O.J.* L 201, 31.7.2002, 37.↩
20. Most notably the Convention on Cybercrime of the Council of Europe (CETS No. 185) – "Budapest Convention".↩
21. As defined in Art. 2(4) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, *O.J.* L 321, 17.12.2018, 36.↩
22. Such as "information society service providers" within the meaning of Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (*O.J.* L 241, 17.9.2015, p. 1).↩
23. Cf. Recital 27 of the Regulation.↩
24. Cf. Recital 28 of the Regulation.↩
25. Art. 3(4) of the Regulation.↩
26. Cf. Recital 30 of the Regulation.↩
27. Recitals 29 and 30 of the Regulation. The same considerations should apply to determine whether a service provider offers services in a Member State.↩
28. It is of note that, according to Art. 1(2) of the Regulation, the suspect or accused person or his lawyer may, under the defence rights afforded to him, request the issuing authority to issue a European Production Order or a European Preservation Order.↩
29. Except the data requested for the sole purpose of identifying the user as defined in Art. 3(10).↩
30. For the definition of the term "emergency cases", see Art. 3(18).↩
31. As defined in Art. 3(10) of the Regulation.↩
32. Directive (EU) 2019/713 of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, *O.J.* L 123, 10.5.2019, 18.↩
33. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA, *O.J.* L 335, 17.12.2011, 1.↩
34. Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, *O.J.* L 218, 14.8.2013, 8.↩
35. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, *O.J.* L 88, 31.3.2017, 6.↩
36. Cf. to this end also Art. 11(4) of the Regulation.↩
37. For details, see below III.2.↩
38. As defined in Art. 3(18) of the Regulation.↩
39. Note: For reasons of clarity and simplicity, explanations in this section III.1 uses the term service provider and not addressee unless it is necessary to distinguish between the two terms. Further details on the designation are provided in section III.2 below.↩
40. Cf. Art. 8(4) of the Regulation.↩
41. Cf. Art. 10(4) of the Regulation.↩
42. Except for data requested for the sole purpose of identifying the user, as defined in Art. 3(10).↩
43. See below III.1 h).↩
44. Art. 8(4) of the Regulation.↩
45. Art. 8(2) and Recital 53 of the Regulation.↩
46. Cf., however, Art. 17(6)(b)(i) in relation to conflicts with the law of a third country, where the nationality is relevant. The language spoken might, however, play a role for the purpose of the rights of defence.↩
47. Art. 12(1)(b) refers to "exceptional situations", "substantial grounds", "specific and objective evidence", "particular circumstances of the case", requiring a "manifest breach". Evidently, the aim is to apply this refusal ground particularly narrowly.↩
48. Enlisted in Annex IV of the Regulation.↩
49. The enforcing authority is also free to raise the grounds of refusal in respect of the Order in its entirety or only in parts.↩
50. Art. 10(2) and (4) of the Regulation.↩
51. See also below III.1 h).↩

52. While the enforcing authority may invoke all the reasons contained in Art. 16(4) and (5), the addressees cannot invoke the reason for a manifest breach of fundamental rights provided for in Art. 16(4)(g) and Art. 16(5)(f), respectively.↩
53. Cf. Art. 1(3) of the Regulation.↩
54. Cf. Recital 16 of the Regulation.↩
55. Art. 13(3) of Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *O.J.* L 119, 4.5.2016, 89.↩
56. Cf. below under III.1. h).↩
57. Cf. Art. 18(2) of the Regulation.↩
58. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *O.J.* L 119, 4.5.2016, 1.↩
59. The service providers are not liable for prejudices to their users or third parties if they act in good faith when complying with the requirements of the European Production Order or the European Preservation Order.↩
60. It should be asked whether delays in the development of the decentralised IT system could constitute such exceptional circumstances.↩
61. Regulation (EU) 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *O.J.* L 257, 28,8.2014, 73.↩
62. Art. 9(2) and (3) of the Regulation provides that the EPOC and the EPOC-PR, respectively, be sent to the service providers containing neither information on necessity and proportionality nor a description of the case.↩
63. Art. 27 of the Regulation. To this end, Member States have to indicate such a decision in a written declaration submitted to the Commission. The Commission will then make the declarations available to all Member States and to the European Judicial Network.↩
64. Opinion of the Legal Research Service of the German Bundestag of 7 February 2011 in the context of data retention ("Die Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta"), WD 11 – 3000 – 12/11.↩
65. Art. 1(1) of the Directive.↩
66. Cf. point 2 in the Explanatory Memorandum of the Commission proposal, COM(2018) 226 final, *op. cit.* (n. 4).↩
67. Art. 2(1)-(3) of the Directive. See also above under III.1.a).↩
68. "Established in the Union" in this context means that there is an entity in the Union that pursues an economic activity for an indefinite period of time through a stable infrastructure from which the business of providing services is carried out or the business is managed, cf. Art. 2(4) of the Directive.↩
69. Situations in which a service provider is established in a Member State and offers services exclusively on the territory of that Member State fall out of the scope of the Directive. Cf. Art. 1(5) of the Directive.↩
70. Art. 2(3) of the Directive. Cf. to this end also III.1.a) above.↩
71. Recital 13 of the Directive.↩
72. *Ibid*.↩
73. *Ibid*.↩
74. Recital 17 of the Directive.↩
75. Cf. Recital 7 of the Directive.↩
76. Cf. Recital 33 of Directive 2014/41/EU regarding the European Investigation Order in criminal matters, *O.J.* L 130, 1.5.2014, 1.↩
77. Convention established by the Council in accordance with Article 34 of the Treaty on the European Union on mutual assistance in criminal matters between Member States of the Union, *O.J.* C 197, 12.7.2000, 3.↩
78. *Ibid*.↩
79. The Directive does not prevent national authorities of a Member State from continuing to address service providers established on their territory for the purpose of gathering electronic evidence in criminal proceedings in purely domestic situations. However, this should not lead to a circumvention of the principles set out in Directive and the Regulation. Cf. Recital 9 of the Directive.↩
80. This applies to the service providers that will begin offering services once the Directive has been transposed and in place for more than six months. Cf. Recital 7 of the Directive.↩
81. Recital 17 of the Directive states that the languages to be used should in any case include one or more of the official languages of the Member State in which the designated establishment is established or the legal representative resides. It may also include other official languages of the Union, such as the language of the headquarters of the service provider.↩
82. For instance, in the case in which the service provider designates several designated establishments or legal representatives. The territory of all the Member States taking part in the instruments within the scope of this Directive should, however, be covered without leaving any gaps. Cf. Recital 17 of the Directive.↩
83. Art 3(5) of the Directive↩
84. Recital 18 of the Directive.↩
85. Cf. Art. 6(3) and Recital 21 of the Directive.↩
86. See, for example, the open letter of 25 organisations, ranging from the Council of Bars and Law Societies of Europe (CCBE) to internet service providers, media, and journalist associations: <https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2021_05_18_EevidenceJointLetter_18May2021.pdf>.↩
87. The most prominent example is the Digital Services Act: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), *O.J.* L 277, 27.10.2022, p. 1.↩
88. Art. 13(3) of Directive (EU) 2016/680 stipulates that "Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to: (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection,

investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; (e) protect the rights and freedoms of others."↩

89. eEvidence: After 5 years of debate European Parliament greenlights agreement | EBU <https://www.ebu.ch/news/2023/06/eevidence-after-5-years-of-debate-european-parliament-greenlights-agreement> accessed 18 September 2023.↩
90. See also: A. Juszczak and E. Sason. "Recalibrating Data Retention in the EU", (2021) *eucrim,* 238-266.↩
91. Art. 25 of the Regulation.↩
92. Agreement on mutual legal assistance between the European Union and the United States of America; *O.J.* L 181, 19.7.2003, 32.↩
93. The Stored Communications Act (SCA), 18 U.S.C. §§ 2701 *et seq.* governs access to stored wire and electronic communications, such as emails and other online messages held by service providers. It forms part of Title II of the Electronic Communications Privacy Act of 1986 (ECPA).↩
94. 18 U.S.C. Chapter 119 – Wire and electronic communications interception and interception of oral communications § 2523. Executive agreements on access to data by foreign governments.↩
95. Landmark U.S.-UK Data Access Agreement Enters into Force | OPA | Department of Justice <https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force>.↩
96. United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime | OPA | Department of Justice <https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime>.↩
97. United States and Canada Welcome Negotiations of a CLOUD Act Agreement | OPA | Department of Justice <https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement>.↩
98. COM(2019) 70 final; Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Council document 10128/19 of 2019-06-12; Addendum to the Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Council document 10128 ADD 1/19 of 2019-06-12↩
99. Addendum to the Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Council document 10128 ADD 1/19 of 2019-06-12; section 3 point 5 (a bis) and (d).↩
100. EU-U.S. announcement on the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations (europa.eu) <https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en>.↩
101. Addendum to the Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Council document 10128 ADD 1/19 of 2019-06-12, paragraph 9 of section II ("nature and scope of the agreement").↩
102. Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework. C(2023)4745 final.↩
103. This includes, for example, the EU Data Act for which political agreement was reached on 28 June 2023 as well as the development of the EU Cybersecurity Certification Scheme on Cloud Services (EUCS).↩
104. Refer to: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.↩
105. Explanatory Report to the Convention on Cybercrime, <https://rm.coe.int/16800cce5b>, para. 16.↩
106. European Council conclusions, 18 October 2018 - Consilium (europa.eu) <https://europa.eu/!gV64YY>.↩
107. Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), COM(2019) 71 final.↩
108. <https://data.consilium.europa.eu/doc/document/ST-9116-2019-INIT/en/pdf>.↩
109. Addendum to the Recommendation for a Council Decision authorising the European Commission to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), 27 May 2019, doc. 9664/19.↩
110. Access to e-evidence: Council authorises member states to sign international agreement - Consilium (europa.eu) <https://europa.eu/!bhYCyR>.↩
111. <https://www.coe.int/en/web/cybercrime/second-additional-protocol>; Malta became the 39th State to sign the protocol on 22 June 2023.↩
112. Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General <https://digitallibrary.un.org/record/1327693?ln=en>.↩
113. The Russian Federation is excluded from the Council of Europe: <https://www.coe.int/en/web/cpt/-/the-russian-federation-is-excluded-from-the-council-of-europe>.↩
114. Press review: Russia unveils bid to fight cyber crime and Samsung Pay faces patent issue – TASS <https://tass.com/pressreview/1320973>.↩
115. United Nations General Assembly, Seventy-fourth session, agenda item 107, Report of the Third Committee, document A/74/401, N1938343.pdf (un.org) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/383/43/pdf/N1938343.pdf?OpenElement>.↩
116. General Assembly Resolution 74/247.↩
117. General Assembly Resolution 75/282.↩
118. Structure of the comprehensive international convention on countering the use of information and communications technologies for criminal purposes, as contained in Annex II to document A/AC.291/7.↩
119. Recommendation for a Council Decision authorising the negotiations for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, COM(2022) 132 final.↩
120. Council Decision (EU) 2022/895.↩
121. *Ibid*. Negotiating directive 27.↩
122. Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/222/255/1E/PDF/2222551E.pdf?OpenElement> and <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V23/039/51/PDF/V2303951.pdf?OpenElement>.↩

123. Most recently, the EU Statement on Article 36 – Protection of personal data (unodc.org) <https://www.unodc.org/documents/Cybercrime/AdHoc-Committee/6th_Session/Informals/Coordinators/230901_EU_statement_on_Art._36.pdf>.↩
124. Available at: <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/CND_2_-_21.04.2023.pdf>.↩
125. These costs are estimated by Cybersecurity Venture; the 2022 Official Cybercrime Report is accessible at: <https://www.esentire.com/resources/library/2022-official-cybercrime-report>.↩
126. Germany, Croatia, Hungary, Poland, and Finland issued an official statement with the adoption of the legislative act. Germany supported the adoption of the Regulation but regretted the lack of clarity as regards the ground for refusal in case of a manifest breach of a fundamental right set out in Art. 6 TEU and in the Charter of Fundamental Rights of the EU and the corresponding recital. Germany also expressed the need for more comprehensive effective remedies, in particular in relation to European Preservation Orders. It also sees a general need to allow for effective remedies not only in the issuing Member State but also in the enforcing Member State. Germany further noted that it considers Recital 53 on the "residence criterion" too vague, particularly the wording on the intention of a person to establish the habitual centre of its interests in a particular Member State as a relevant objective circumstance to determine his/her residence; the wording leaves too much room for interpretation and thus extends the scope of this criterion. Hungary and Poland objected to the inclusion of Art. 7(1) TEU in a recital related to the ground for refusal of European Production Orders in case of a manifest breach of a fundamental right set out in Art. 6 TEU and in the Charter of Fundamental Rights of the EU. Although Croatia expressed its dissatisfaction with the linguistic version of the proposals, it generally welcomed the adoption of the legislative acts. Finland voted against the adoption of the Regulation, reasoning that a judicial assessment should also be carried out by the competent authorities in the enforcing State for European Production Orders issued in relation to the most sensitive data. Finland also regretted that the grounds for refusal do not include a ground allowing the enforcing authority to refuse a production order for traffic and content data in cases in which the use of such a measure is restricted under the law of the enforcing State to certain offences or to offences punishable by a certain minimum threshold.↩

Authors statement

The views expressed in this article are solely those of the authors and are not an expression of the views of their employer or the institution they are affiliated with.

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