Seirbhís Leabharlainne 7 Taighde
Library & Research Service

Briefing Paper

International cooperation on electronic evidence in criminal proceedings

Implications of the EU e-Evidence Package

Karen McLaughlin
Senior Parliamentary Researcher (Law)

25 May 2026

Policy and Legislative Briefing Paper

Abstract

This paper provides an overview of the EU's e-Evidence package (consisting of Regulation (EU) 2023/1543 and Directive (EU) 2023/1544). It notes the increased use of electronic evidence in criminal trials and the large volume of service providers based in Ireland as key policy drivers. It also outlines the domestic and international legislative context, including the Budapest Convention and UN Convention against Cybercrime. Lastly, the paper traces the potential implications of the Government's forthcoming legislative proposals which will give effect to the e-Evidence package, including the proposed establishment of the Criminal Justice International Cooperation Office.

Tithe an Oireachtais
Houses of the Oireachtas

Library & Research Service

Email: library.and.research@oireachtas.ie

This L&RS publication may be cited as:

Oireachtas Library & Research Service, 2026. Policy and Legislative Briefing Paper: International cooperation on electronic evidence in criminal proceedings: Implications of the EU e-Evidence Package.

Legal Disclaimer

Contact

Houses of the Oireachtas
Leinster House
Kildare Street
Dublin 2
D02 XR20

Tel: +353 (0)1 6183000
Twitter/X: @OireachtasNews

www.oireachtas.ie

Executive Summary

Electronic information is now heavily relied upon as evidence in criminal proceedings. International cooperation on electronic evidence has traditionally involved mutual legal assistance measures which have been found to be too slow and ineffective.

The EU's e-Evidence package will allow for authorities in one EU Member State to issue orders requiring either the production or preservation of data held by service providers in another EU Member State without needing additional judicial approval from the service provider's home country. This procedure has been developed to speed up the process since electronic data can be moved, amended or erased quickly. Service providers are required to designate legal representatives to receive these orders and must either produce or preserve the data within specific timeframes. Enforcement authorities will be responsible for compliance with the orders and may impose penalties of up to 2 per cent of the service provider's total worldwide annual turnover in the preceding financial year. The enforcing authority may also object to an order on various grounds, including a manifest breach of fundamental rights.

Cross-border cooperation on electronic evidence in criminal proceedings is shaped by EU and international law and sees the intersection of criminal procedure, the law of evidence, data protection and human rights law. While the EU e-Evidence package consists of two instruments (Regulation (EU) 2023/1543 and Directive (EU) 2023/1544), this area is also impacted by domestic law and international instruments, including the Budapest Convention and UN Convention against Cybercrime.

Given that this cooperation involves service providers, the operation and regulation of the digital services sector is a significant factor in the policy context. In the context of the Irish sector, it is anticipated that service providers based in Ireland will receive in excess of 300,000 orders per annum. This will have potential implications for the proposed new body, which is to be established by forthcoming legislation, namely the Criminal Justice International Cooperation Office (CJICO). While the Office will start receiving orders by 18 August 2026, which is the date when the e-Evidence Regulation will apply, it is anticipated that the office will comprise 150 staff working across four divisions by 2028.

During pre-legislative scrutiny, concerns were raised about the financial and human resources to be allocated to the CJICO as well as a lack of transparency as to how the State and providers will handle requests for data. In addition, the Joint Oireachtas Committee on Justice, Home Affairs and Migration raised a number of fundamental rights concerns, including a lack of safeguards and incentives for service providers to consider data protection rights and fundamental rights. This concern was echoed by an academic who made a written submission to the Committee further to a request. The Courts Service expressed concern that appeals may require significant court time, particularly where penalties involve substantial sums of money.

Both the Criminal Justice (International Cooperation Office) Bill and the Criminal Justice (Protection, Preservation of and Access to Data) Bill have been listed as priority for publication in the Government's Summer Legislation Programme.

Contents

Introduction

International cooperation in criminal proceedings has traditionally taken place through mutual legal assistance. Mutual legal assistance involves requests for assistance from one state to another in relation to criminal investigations or proceedings. This paper focuses on international cooperation in relation to accessing electronic or digital information, which is now heavily relied upon as evidence in criminal proceedings. This is a complex area that sees the intersection of various areas of law including criminal procedure, the law of evidence, data protection and human rights law. This area is also heavily influenced by European Union (EU) law and international law.

In particular, this paper will examine the implications of the implementation of the EU's e-Evidence package on Irish law. The EU e-Evidence package was developed to make it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence required to investigate and prosecute crimes. The EU's e-Evidence Package consists of Regulation (EU) 2023/1543[1] and Directive (EU) 2023/1544[2]. These EU instruments will be given effect by the following legislative proposals:

- Criminal Justice (International Cooperation Office) Bill
- Criminal Justice (Protection, Preservation and Access to Data on Information Systems) Bill

The purpose of this paper is to consider the policy and legislative background to the EU's e-Evidence package as it relates to the Government's legislative proposals. It will also outline how the Government's legislative proposals may lay the foundation for the ratification of international agreements and the application of other EU instruments.

The PRS has also produced Bill Resource Pages on the Criminal Justice (International Cooperation Office) Bill and Criminal Justice (Protection, Preservation and Access to Data on Information Systems) Bill which provide links to a wide range of sources on the Bill, including stakeholder and academic commentary (available internally only).

[1] 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.
[2] 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.

Policy Context

Electronic evidence in criminal proceedings

Reflecting on the impact of information and communications technologies on criminal proceedings, Franssen and Tosza conclude that these interactions leave "precious digital traces that could be used as evidence" in criminal proceedings and note: [3]

> *In nearly every criminal investigation, LEAs [law enforcement authorities] are confronted with perpetrators and/or victims who used an electronic device and/or communicated in some way through the internet (via email, voice over internet protocol (VoIP) or internet telephony, chat sessions or online games, private messaging applications or social media).*[4]

This type of evidence is referred to as digital or electronic evidence[5]. The European Union estimates that "around 85% of criminal investigations now rely on law enforcement authorities' ability to access digital information". [6]

Franssen and Tosza identify the following issues in the collection of such evidence:

1. existing investigative tools and powers do not always keep pace with technology,
2. data is volatile due to a range of factors including its location of storage, which may change over time, and
3. companies providing such technologies, often referred to as 'service providers', use security-enhancing techniques to protect the privacy and data of their users.[7]

The European Commission has also recognised that electronic evidence is generally only available on private infrastructures, which "may be located outside the investigating country, owned by service providers established outside the investigating country, or both."[8] Franssen

---

[3] Franssen, V. and Tosza, S. (2025) 'Introduction: Gathering Electronic Evidence and Cooperation with Service Providers in the Digital Era – A Jigsaw Puzzle of Technological and Legal Challenges', in V. Franssen and S. Tosza (eds.) *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge: Cambridge University Press (Cambridge Law Handbooks), pp 1–10.

[4] Ibid, p 1.

[5] The legal definition of 'electronic evidence' in the context of the EU e-Evidence package will be discussed later in this paper.

[6] European Commission (2025) *ProtectEU: a European Internal Security Strategy*, Strasbourg, 1.4.2025 COM(2025) 148 final.

[7] Franssen, V. and Tosza, S. (2025) 'Introduction: Gathering Electronic Evidence and Cooperation with Service Providers in the Digital Era – A Jigsaw Puzzle of Technological and Legal Challenges', in V. Franssen and S. Tosza (eds.) *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge: Cambridge University Press (Cambridge Law Handbooks), pp 1–10.

[8] European Commission (2018) Impact Assessment of the E-Evidence package, SWD(2018) 118 final.

and Tosza note that this requires cooperation between law enforcement authorities and private actors and describe the scenario as follows:

> *When a service provider is located in another country, or when the data is stored abroad, LEAs should in principle resort to mutual legal assistance (MLA) because their coercive powers are limited to their national territory. The MLA rules are designed to facilitate judicial cooperation between states to gather or exchange information for law enforcement purposes.*[9]

In addition, the European Commission has identified a wide range of stakeholders who are affected by the challenges in cross-border access to e-Evidence in criminal matters, which may be summarised as follows:

- **Society in general**: ineffective investigation and prosecution of crime may damage the rule of law and general security.
- **Victims of crime:** delayed investigation and prosecution of the crime can lead to a range of negative consequences (e.g. economic, physical, psychological)
- **Suspects in criminal investigations**: fundamental rights and procedural fairness must be respected during criminal investigations and prosecutions
- **Users of the services offered by service providers**: fundamental rights of service users may be affected in the course of criminal investigations.
- **Service providers**: responding to requests is resource intensive.
- **Public authorities** (including the judiciary and law enforcement) may issue requests for access to electronic evidence as well as respond to requests for such evidence.[10]

The European Commission's Impact Assessment of the e-Evidence package summarised the issues connected with electronic evidence in criminal proceedings as follows:

- judicial cooperation is often too slow for timely access to data and can entail a disproportionate expense of resources;
- direct cooperation can be unreliable, is only possible with a limited number of service providers which all apply different policies, is not transparent and lacks accountability;
- legal fragmentation abounds, increasing costs on all sides; and
- the size of the problem is steadily increasing, creating further delays.[11]

---

[9] Franssen, V. and Tosza, S. (2025) 'Introduction: Gathering Electronic Evidence and Cooperation with Service Providers in the Digital Era – A Jigsaw Puzzle of Technological and Legal Challenges', in V. Franssen and S. Tosza (eds.) *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge: Cambridge University Press (Cambridge Law Handbooks), pp 1–10.

[10] European Commission (2018) Impact Assessment of the E-Evidence package, SWD(2018) 118 final, p 21.

[11] European Commission (2018) Impact Assessment of the E-Evidence package, SWD(2018) 118 final.

The Commission also notes that "the fact that some crimes cannot be effectively investigated and prosecuted in the EU is a problem because it results in criminals enjoying impunity, victims being less protected and EU citizens may feel increasingly threatened by criminal activity".[12]

The Commission concludes that the objective of the e-Evidence package:

> *... is to ensure effective investigation and prosecution of crimes in the EU by improving cross-border access to electronic evidence through enhanced judicial cooperation in criminal matters and an approximation of rules and procedures.*

Digital services sector and regulation in Ireland

In the recruitment advertisement for the Director of the Criminal Justice International Cooperation Office, it is stated:

> *Given the number of large service providers based in Ireland, the e-Evidence Package will have significant implications for Ireland's tech sector and criminal justice system. Successful implementation of the EU e-Evidence Package will also have a major strategic impact on Ireland's reputation as a hub for digital regulation, and on its ability to ensure effective access to digital evidence in tackling serious crime. Given the anticipated scale of orders being addressed to service providers based in Ireland, effective implementation of the e-Evidence Package is also key to the successful operation of the e-Evidence system across the EU.*

The latest data from the EU's SIRIUS project[13] demonstrates an increase in EU data requests to service providers by 22 per cent, from 2022 to 2023.[14] Figure 1 below breaks down the data requests sent to service providers by company in 2023.

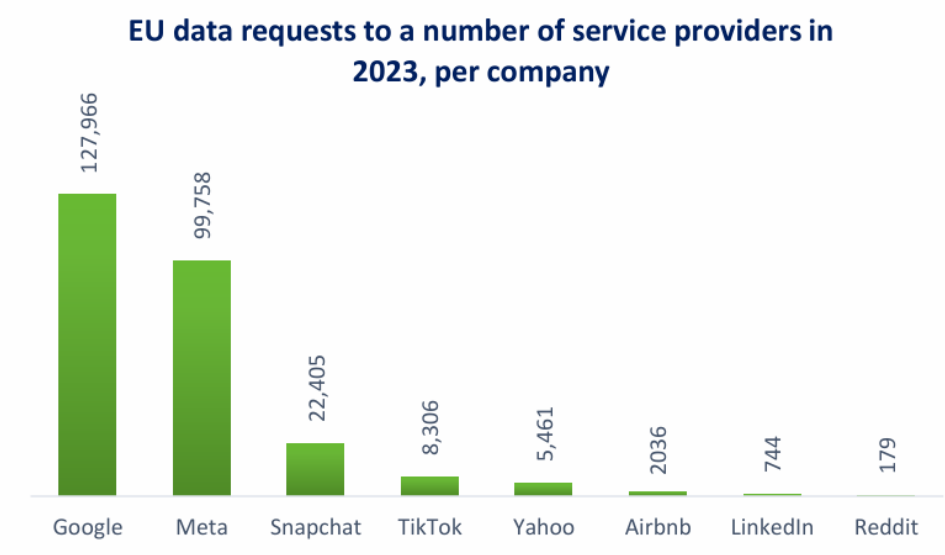
---

[12] European Commission (2018) Impact Assessment of the E-Evidence package, SWD(2018) 118 final.

[13] The SIRIUS Project is an established centre of excellence in the field of cross-border access to electronic evidence in the EU. Implemented by Europol and Eurojust, the project assists over 7,800 law enforcement officers and over 550 judicial authorities from all 27 EU Member States, as well as 23 third countries, in the process of requesting data from service providers, in the context of criminal investigations.

[14] European Union Agency for Law Enforcement Cooperation and European Union Agency for Criminal Justice Cooperation (2024) 6th Annual SIRIUS EU Electronic Evidence Situation Report, p 53.

Figure 1: EU data requests to select service providers in 2023, by company



Source: SIRIUS e-Evidence Situation Report 2024, p. 54.

Of all the companies listed in Figure 1 above, Snapchat and Reddit are the only companies that do not have their European headquarters in Dublin.

In a 2025 speech by Minister for Justice, Home Affairs and Migration, Jim O'Callaghan TD, stated:

> *We are a digital hub within Europe and home to many of the largest global tech companies, as well as small to medium service providers. This brings many opportunities and benefits, certainly to the Irish economy, but also what comes with it, our responsibility. For that reason, how Ireland implements this framework will have consequences not only for our justice system, but for digital governance across the EU.*[15]

In its National Digital Strategy, the Government outlined Ireland's commitment to "continue to provide a modern, cohesive and well-resourced digital regulatory system". In its 2024 progress report, the Government listed preparations for the implementation of the EU e-Evidence Package as a deliverable under this workstream.[16]

---

[15] Strengthening Justice in the Digital Age: Ireland's Leadership under the EU e-Evidence Regulation. This was the keynote speech delivered by the Minister at the iTrust6A symposium on 'The Impact and Importance of the EU's e-Evidence Regulation for Ireland'. The event was held on 22 October 2025 at the European Parliament Liaison Office on 11 Chatham Street.

[16] Department of An Taoiseach (2025) Harnessing Digital The Digital Ireland Framework 2024 Progress Report, p 5.

Legal Context

This section of the Paper will provide an outline of the EU e-Evidence Package as well as an overview of the existing domestic legal framework and related EU and international instruments.

Existing domestic legal framework

Cooperation in criminal justice matters

Ireland currently participates in a range of European Union mutual assistance initiatives including Europol, Eurojust, the European Arrest Warrant, mutual assistance, the European Criminal Reports Information System, the Schengen Information System (SIS II).[17]

However, Daly and Heffernan note that Ireland does not participate in other measures such as the European Investigation Order and the European Public Prosecutors Office[18] and suggest that this may be "attributable in part to concerns about the adaptability of largely continental-inspired measures to our common law adversarial trial system".[19] It should be noted that Ireland does not automatically participate in justice and home affairs initiatives of the EU and must instead opt-in to measures in accordance with Protocol 21 to the Treaty on the Functioning of the European Union (TFEU).[20] In a Review of the operation of Protocol 21 it was suggested that the Department of Justice should give consideration to participation in justice and home affairs measures by default.[21]

---

[17] Heffernan and Daly (2025) "Background." in *Evidence in Criminal Trials*, London Dublin: Bloomsbury, para 1.06.

[18] Ireland chose not to opt in to membership of the European Public Prosecutor's Office, an independent body established in 2017 to investigate crimes against the financial interests of the EU and the participating states. These crimes are as set out in Directive (EU) 2017/1371 of the European Parliament and of the Council on the fight against fraud to the Union's financial interests by means of criminal law, otherwise known as the PIF Directive, which has been transposed by Ireland. According to a response to Parliamentary Question No. 3140/25: "In October 2023, the Government approved the drafting of the General Scheme of legislation to allow Ireland to join EPPO. This detailed preparatory work will take some time to complete before the Government makes a formal decision to join EPPO." The relevant legislative proposal appears on the 'All Other Legislation' section of the Summer Legislation Programme 2026.

[19] Heffernan and Daly (2025) "Background." in *Evidence in Criminal Trials*, London Dublin: Bloomsbury Publishing Plc. Accessed April 17, 2026, para 1.06.

[20] This area is formally known as Title V of the TFEU, which is entitled the 'Area of freedom, security and justice'.

[21] Department of Justice (2024) PROTOCOL 21 Review of Ireland's Protocol on the area of freedom, security and justice, p 84.

The Criminal Justice (Mutual Assistance) Act 2008 gives effect to some of the EU's justice and home affairs measures in relation to mutual assistance, including the following:

- Information about Financial Transactions for Criminal Investigation Purposes (Part 2)
- Interception of Telecommunications Messages (Part 3)
- Freezing, Confiscation and Forfeiture of Property (Part 4)
- Financial Penalties (Part 4A)
- Provision of Evidence (Part 5)

The Act also covers mutual assistance in criminal matters between Ireland and the United States of America (Part 7), as well as the European Public Prosecutor's Office (EPPO) (Part 7B). The Act also contains provisions related to the exchange of information concerning terrorist offences between Europol, Eurojust and member states.

This Act also gives effect to the European Convention on Mutual Legal Assistance in Criminal Matters (1959) and two of its Additional Protocols. Ireland ratified the Convention and its Additional Protocol (1978) on 28 November 1996 and it entered into force on 26 February 1997. Ireland ratified the Second Additional Protocol to the Convention on 26 July 2011 and it entered into force on 01 November 2011. The Convention is an instrument of the Council of Europe whereby parties agree to afford each other the widest measure of mutual assistance with a view to gathering evidence, hearing witnesses, experts and prosecuted persons, etc.

Access to data

According to McIntyre and Murphy:

> *... despite the importance of this [technology] sector to the Irish economy, there is little legislation in Ireland which deals with cross-border access to data or indeed access to data generally.*[22]

Furthermore, the authors note that in the absence of a comprehensive legal framework in this area, both Irish law enforcement authorities and those based in other countries have relied

[22] McIntyre TJ, Murphy MH. Accessing Digital Evidence in Criminal Matters: An Inadequate Irish Legal Framework. In: Franssen V, Tosza S, eds. *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge Law Handbooks. Cambridge University Press; 2025:309-346. TJ McIntyre is a leading author and activist in this area and provided this chapter and a written submission to the Joint Oireachtas Committee on Justice, Home Affairs and Migration in response to a request from the Committee in its pre-legislative scrutiny of the General Scheme of the Criminal Justice (International Cooperation Office) Bill.

upon voluntary disclosure of data which is held by service providers based in Ireland.[23] The authors suggest that this decreases transparency and ensures that, "in many cases there is a lack of fundamental rights safeguards against abuse".[24]

McIntyre and Murphy also outline developments in Irish telecoms data retention law[25], including a successful challenge in the Court of Justice of the European Union[26] and subsequent amendments to address the ruling.[27] Nevertheless, McIntyre and Murphy express concerns about the legality of the current regime.[28] In its first Annual Report, the Independent Examiner of Security Legislation noted that "the striking feature of the legislation is the absence of a general obligation to retain data for the purpose of access in the course of investigations of serious crime". Nevertheless, the Examiner noted such a requirement is not possible given the judgments of the Court of Justice of the European Union.[29]

The European Commission is currently considering proposals for a new legislative framework in relation to data retention in the EU. A General Scheme of a Communications (Retention of Data) Bill was published in 2017. This Bill remained on successive Government Legislation Programmes until the Spring Legislation Programme 2026, when the reference to the Bill was removed.

While there may not be a comprehensive framework on access to data there are a range of search, seizure and production powers in relation to records held on paper or computers, including:

- Search warrants (Criminal Justice (Search Warrants) Act 2012),
- Orders to make material available (section 63 Criminal Justice Act 1994 and section 14A of the Criminal Assets Bureau Act 1996),
- Orders to produce documents or provide information (Criminal Justice Act 2011).
- Powers to seize computers and records, to operate computers at the place being searched, to require disclosure of passwords or encryption keys from a person at the place being searched and to require information stored on a computer to be produced in a visible and legible form (section 7 of the Criminal Justice (Offences Relating to Information Systems) Act 2017).

---

[23] Ibid.

[24] Ibid.

[25] Communications (Retention of Data) Act 2011.

[26] Case C-140/20, *G.D.* v. *Commissioner of An Garda Síochána and others* [2022]

[27] Communications (Retention of Data) (Amendment) Act 2022. See L&RS Bill Digest on the Communications (Retention of Data) (Amendment) Act 2022.

[28] McIntyre TJ, Murphy MH. Accessing Digital Evidence in Criminal Matters: An Inadequate Irish Legal Framework.

[29] Office of the Independent Examiner of Security Legislation (2026) Annual Report of the Independent Examiner of Security Legislation, pp 42-60.

Data protection

Article 8 of the European Charter of Fundamental Rights protects the right to data protection. The General Data Protection Regulation (GDPR)[30] acts as *lex generalis* (general law) for data protection in the EU. Two other specialist EU Directives (*lex specialis)* are relevant in the context of this area, namely the Law Enforcement Directive[31] and the ePrivacy Directive.

It should be noted that on 7 May 2026, the European Parliament and the Council of the EU reached a provisional agreement on the AI component of the Digital Omnibus package. However, the parallel proposals to amend the digital acquis, including the GDPR and the ePrivacy Directive, remain unfinalised in the legislative pipeline.[32] Given that this legal instrument has not yet been finalised it is not clear what, if any, impact this may have on the implementation of the EU e-Evidence package.

The Data Protection Act 2018 gave effect to both the General Data Protection Regulation (GDPR)[33] and the Law Enforcement Directive.[34] The ePrivacy Directive was also transposed into the Irish law by the ePrivacy Regulations[35]. Section 71(1) of the Data Protection Act 2018 stipulates that when processing personal data for law enforcement purposes[36], the data must be:

- processed fairly and lawfully;
- collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected;
- accurate, kept up to date if necessary, and every reasonable step should be taken to ensure (with due regard to the purpose they were collected) inaccurate data are rectified or erased;
- kept in a form that permits the identification of a data subject for no longer than is necessary for the purposes for which the data are collected;

---

[30] Regulation (EU) 2016/679. This Regulation applied from 25 May 2018.
[31] Directive (EU) 2016/680.
[32] See EU agrees to simplify AI rules to boost innovation and ban 'nudification' apps to protect citizens and Provisional agreement reached on the Digital Omnibus on AI - DETE. For further discussion of the proposals see L&RS Blog on the EU Digital Omnibus Package | Resources for Members, published 24 November 2025 [internal access only].
[33] Regulation (EU) 2016/679. This Regulation applied from 25 May 2018.
[34] Directive (EU) 2016/680.
[35] European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 SI No. 336 of 2011,
[36] This relates to the processing of personal data by data controllers who are competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, where personal data is being processed for these purposes.

- processed in a manner that ensures appropriate security of the data against unauthorised or unlawful processing and accidental loss damage or destruction.

Robinson has noted that while data protection is not routinely cited in the e-Evidence Package, there is potential for conflict with established rules in relation to data controllers and processors, which may lead to the "dilution or even circumvention of data subject rights".[37]

[37] Robinson, G. (2025) 'Effective Data Protection and Direct Cooperation on Digital Evidence', in V. Franssen and S. Tosza (eds.) *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge: Cambridge University Press (Cambridge Law Handbooks), pp. 68–103.

EU e-Evidence Package

Article 82(1) of the Treaty on the Functioning of the European Union (TFEU) provides that "Judicial cooperation in criminal matters in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions". This was first given effect in the Framework Decision on the European Arrest Warrant[38] and has since regulated other scenarios of judicial cooperation in criminal matters within the EU, including the e-Evidence package.

While these new instruments will be available under the e-Evidence package, investigators will be free to use other EU or international mutual recognition instruments.[39] The development of the e-Evidence package comes from a recognition that:

> *Member States' authorities should choose the tool most adapted to the case at hand. In some cases, they might prefer to use Union and other international instruments, agreements and arrangements when requesting a set of different types of investigative measures that are not limited to the production of electronic evidence from another Member State.*[40]

In light of this, both related EU instruments and international instruments will be outlined later in this Paper following an overview of the e-Evidence package.

Commentators have noted that the package represents "a major paradigm shift" as for the first time, national investigating authorities will be able to make a direct request to service providers in other member states to hand over or secure electronic evidence, which the service providers must comply with.[41] The EU e-Evidence package consists of the:

- Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (Regulation (EU) 2023/1543) and,
- Directive (EU) 2023/1544 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.

The Regulation will apply directly to Ireland as a consequence of Ireland opting into the measure under Protocol 21 to the TFEU, while the Directive requires domestic transposition.

---

[38] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.7.2002, 1.

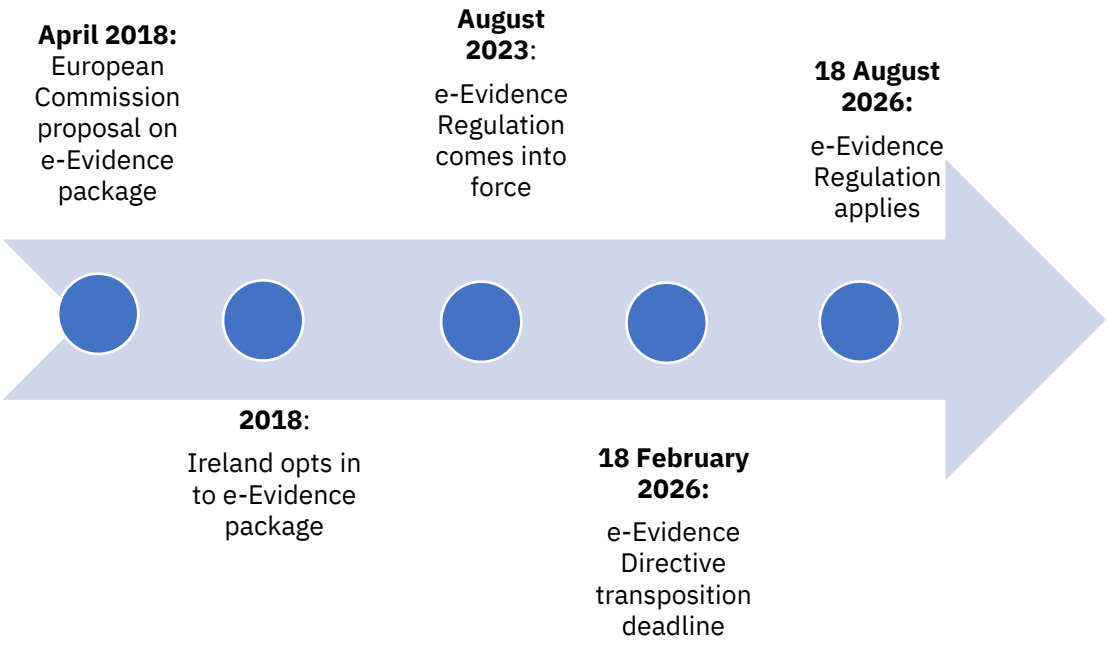
[39] These instruments are discussed later in this paper.

[40] Recital 96 of the e-Evidence Regulation. See also: Ramos (2025) European Preservation and Production Orders: A Non-Exclusive Approach to E-Evidence within the EU, EUCrim, 'Current Challenges for Judicial Cooperation', 2025/3, pp 216-220.

[41] Christakis, T. (2025) 'From Mutual Trust to the Gordian Knot of Notifications: The EU e-Evidence Regulation and Directive', in V. Franssen and S. Tosza (eds.) *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge: Cambridge University Press (Cambridge Law Handbooks), pp. 173–199.

As can be seen below, the package has been in development since 2018 and will come into effect in 2026.

Figure 2: EU e-Evidence Package – Development to application



Source: PRS (2026)

It should be noted that the European Commission has instigated infringement proceedings against Ireland in respect of its failure to transpose Directive 2023/1544 on time, issuing a letter of formal notice on 26 March 2026.[42]Ireland is required to designate one or more central authorities to ensure that Directive 2023/1544 is applied in a consistent and proportionate manner as well as ensuring cooperation between authorities and the European Commission, where required.[43]

Regulation (EU) 2023/1543 also provides that Member States may designate one or more central authorities to be responsible for the administrative transmission of European Preservation and Production Orders and Certificates as well as for the receipt of data and notifications and the transmission of other official correspondence relating to such certificates or orders.

[42] An explanation of infringement proceedings is available here.

[43] Article 6 of Directive 2023/1544.

European Production or Preservation Orders

The Regulation provides for two new measures to be introduced across the European Union for the purpose of obtaining electronic evidence in criminal proceedings, namely:

1. **European Production Order :** will allow law enforcement authorities in one EU Member State to request electronic data from service providers (established or represented in another EU Member State), which are compelled to provide the data requested. The order is transmitted using a European Production Order Certificate (EPOC).
2. **European Preservation Order**: can be issued by law enforcement authorities to oblige service providers to preserve electronic data that can later be requested for production, so that the data are prevented from being deleted or altered. The order is transmitted using a European Preservation Order Certificate (EPOC-PR).

The Regulation also provides that a suspect or an accused person (or his/her lawyer) can request the issuing of a European Production or Preservation Order "within the framework of applicable defence rights in accordance with national criminal procedural law".

The Regulation sets out rules for the issuing and execution of these instruments as well as grounds for refusal and enforcement and penalties procedures by the enforcing authority. The Regulation also provides for a review procedure in the case of conflicts of laws and a decentralised IT system.

The Regulation applies to service providers which offer services in the European Union. 'Service providers' are defined in the Regulation as individuals or 'legal persons', such as companies, providing one or more of the following services:

- 'electronic communications services'[44], including[45]:
  - 'internet access service'[46]
  - interpersonal communications service; and
  - services relating to the transmission of signals, e.g. broadcasting;
- internet domain name and IP numbering services, such as IP address assignment, domain name registry, domain name registrar and domain name-related privacy and proxy services;
- 'information society services'[47] that:
  - enable their users to communicate with each other; or

[44] As defined in Article 2(4) of Directive (EU) 2018/1972.
[45] Services providing, or exercising editorial control over, content transmitted using electronic communications networks and services are excluded from this definition.
[46] Article 2(2) of Regulation (EU) 2015/2120 as which includes a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used.
[47] Article 1(1)(b) of the Technical Regulations Information System (TRIS) Directive (EU) 2015/1535.

- make it possible to store or otherwise process data on behalf of the users to whom the service is provided, provided that the storage of data is a defining component of the service provided to the user;

Financial service providers, such as banking, credit, insurance and re-insurance, occupational or personal pensions, securities, investment funds, payment and investment advice[48], are exempt from this definition.[49]

'Electronic evidence' is categorised into different data types which are stored electronically by or on behalf of a service provider, at the time of the receipt of a EPOC or a EPOC-PR. These are set out in Box 1 below.

Box 1: Data Categories under the Regulation (Article 3)

- **subscriber data:** any data related to the identity of a subscriber or customer (e.g. name, date of birth, postal or geographical address, billing and payment data, telephone, or email); or the type of service provided to the subscriber or customer and its duration;
- **user identification data:** IP addresses and, where necessary, the relevant source ports and time stamp, namely the date and time, or technical equivalents of those identifiers and related information, where requested by law enforcement authorities or by judicial authorities for the sole purpose of identifying the user in a specific criminal investigation;
- **traffic data:** data related to the provision of a service offered by a service provider that serve to provide context or additional information about such service and are generated or processed by an information system of the service provider (e.g. metadata, location data);
- **content data:** any data other than subscriber or traffic data stored in a digital format such as text, voice, videos, images, and sound.

[48] Including the services listed in Annex I to Directive 2006/48/EC.
[49] Article 3(3) of Regulation (EU) 2023/1543.

Issuing European Production and Preservation Orders (Articles 4-6)

The question of who is authorised to issue a European Production Order or a European Preservation Order depends on the instrument and the category of data requested. It is suggested that:

> *... 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.*[50]

Table 1 below provides an overview of the issuing authority for different types of European Production and Preservations Orders.

Once a European Production Order or a European Preservation Order has been validated by a judicial authority, that authority will be regarded as the "issuing authority" for the purposes of transmission of a European Production Order Certificate (EPOC) and European Preservation Order Certificate (EPOC-PR). Annex I and II of the Regulation provide for standardised certificates for EPOCs and EPOC-PRs, respectively.

Table 1: Overview of conditions for issuing European Production and Preservation Orders

Instrument	Type of data	Applicable criminal offences	Issuing authority
European Production Order	subscriber data user identification data	all criminal offences, and the execution of a custodial sentence or a detention order of at least four months where the person convicted absconded from justice.	a judge, a court, an investigating judge or a public prosecutor competent in the case concerned; or any other competent authority, provided the order has been validated by a judicial authority.

[50] Juszczak (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* Issue 2/2023, pp 182-200.

Instrument	Type of data	Applicable criminal offences	Issuing authority
European Production Order	traffic data content data	criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least three years; certain fraud offences[51]; offences concerning sexual abuse, exploitation, child pornography and solicitation of children[52] offences related to illegal system access, data interference and interception;[53] certain terrorist offences;[54] or the execution of a custodial sentence or a detention order of at least four months.	a judge, a court or an investigating judge competent in the case concerned; or any other competent authority, provided the order has been validated by a judicial authority.
European Preservation Order	Any data	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.	a judge, a court, an investigating judge or a public prosecutor competent in the case concerned; or any other competent authority as defined by the issuing State, provided the order has been validated by a judicial authority.

Source: PRS (2026), based on Regulation (EU) 2023/1543.

[51] Offences as defined in Articles 3 to 8 of Directive (EU) 2019/713.

[52] Offences as defined in Articles 3 to 7 of Directive 2011/93/EU.

[53] Offences as defined in Articles 3 to 8 of Directive 2013/40/EU.

[54] Criminal offences as defined in Articles 3 to 12 and 14 of Directive (EU) 2017/541.

Emergency cases

The Regulation also provides that in emergency cases 'competent authorities' may issue a European Production Order or a European Preservation Order, subject to certain conditions, without prior judicial validation. An 'emergency case' is defined as:

> *... a situation in which there is an imminent threat to the life, physical integrity or safety of a person, or to a critical infrastructure, as defined in Article 2, point (a), of Directive 2008/114/EC, where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State;*[55]

An order may be issued by competent authorities in such cases where validation cannot be obtained in time and where those authorities could issue an order in a similar domestic case without prior validation. Where such an order has been issued, *ex post* validation must be sought within 48 hours at the latest and where such validation is refused, the order should be immediately withdrawn.

Conditions attached to European Production and Preservation Orders

Articles 5 and 6 of the Regulation specify the conditions for issuing the European Preservation and Production Orders, including:

- **Necessity and proportionality:** orders may only be issued where necessary and proportionate, considering the rights of the suspect or the accused person;
- **Domestic equivalence:** orders may only be issued if a similar order could have been issued under the same conditions in a similar domestic case;
- **Privileges and immunities[56]:** European Production Orders for traffic or content data may not be issued if protected by immunities and privileges or rules regarding freedom of expression and freedom of the press in the enforcing State.

[55] Article 3(18) of theRegulation (EU) 2023/1543

[56] Article 5(10) of Regulation (EU) 2023/1543.

Service provider obligations

Regulation (EU) 2023/1543 and Directive (EU) 2023/1544 require service providers to designate or appoint at least one "addressee" for the receipt of, compliance with and enforcement decisions and orders for the purpose of gathering electronic evidence. This is a core requirement of the EU e-Evidence package which allows for European Production Order and European Preservation Orders to be addressed directly to service providers[57] rather than having to go through court processes, which is the case with other mutual assistance mechanisms. Member States are obliged to develop penalties for service providers who fail to appoint addressees.[58]

Service providers must act quickly and produce the requested data within set timeframes as follows:

- The requested data must be produced to the issuing authority or law enforcement authorities within **10 days** upon receipt of a **European Production Order Certificate**, provided no grounds for refusal has been raised by the enforcement authority [59]
- In emergency cases, the requested data must be transmitted without undue delay and at the latest within **eight hours** following receipt of the EPOC.
  Data must be preserved without undue delay and kept for **60 days,** when a **European Preservation Order** has been issued. The issuing authority may also extend the preservation period for an additional **30 days.**

The service provider must ensure confidentiality, secrecy and integrity of the data produced and preserved.[60]Service providers may raise objections to European Production or Preservation Orders on the basis of immunities, privileges and/or conflict of laws.[61] Issuing and enforcing authorities must be informed of such objections.[62]

---

[57] Article 7 of Regulation (EU) 2023/1543.

[58] Articles 3-5 of Directive (EU) 2023/1544.

[59] Article 10 of Regulation (EU) 2023/1543.

[60] Article 13(4) of Regulation (EU) 2023/1543.

[61] Articles 12 and 17, respectively, of Regulation (EU) 2023/1543.

[62] Articles 10-11 of Regulation (EU) 2023/1543.

Role of enforcing authority

The 'enforcing authority' is defined as the body in the 'enforcing State'[63] which is "competent to receive a European Production Order and an EPOC or a European Preservation Order and an EPOC-PR transmitted by the issuing authority for notification or enforcement" in accordance with Regulation (EU) 2023/1543. The Regulation sets out two separate roles for the enforcing authority.

Firstly, the enforcing authority must be notified of European Production Orders to obtain traffic data or content data.[64] This notification is not required where the person whose data is sought is a resident of the issuing state and has committed or is likely to commit an offence. Having reviewed the order, the authority may either raise grounds for refusing the order or ensure enforcement of legitimate orders.[65] Orders may be refused on the following grounds:

- Immunities and privileges,
- Manifest breach of fundamental rights,
- *Ne bis in idem* (double jeopardy),[66]
- Double criminality.

Grounds for refusal must be raised within 10 days following receipt of the notification in regular cases, and 96 hours following such receipt in emergency cases. Before deciding to raise a ground for refusal, the enforcing authority must contact the issuing authority and negotiate a solution.

Secondly, the regulation provides that the issuing authority must notify the enforcement authority of non-compliance with orders made under the regulation. The enforcement authority may impose penalties of up to 2 per cent of the service provider's total worldwide annual turnover in the preceding financial year.[67] Member States must also report non-compliant service providers to the European Commission annually under the Directive.

---

[63] 'Enforcing State' is defined in Article 3(16) of Regulation (EU) 2023/1543 as "the Member State in which the designated establishment is established or the legal representative resides and to which a European Production Order and an EPOC or a European Preservation Order and an EPOC-PR are transmitted by the issuing authority for notification or for enforcement in accordance with this Regulation".

[64] Article 8.1 of the Regulation provides that the enforcing authority must be notified of EPOs to obtain traffic data or content data by the issuing authority.

[65] The enforcing authority must ensure enforcement of legitimate orders in accordance with the detailed rules stipulated in Article 16 of the Regulation (EU) 2023/154.

[66] According to Murdoch and Hunt's Encyclopedia of Irish Law this relates to "The common law doctrine that a person should not face repeated prosecution for the same offence. However, he may be charged with different offences arising out of the same act, whether of commission or omission, but usually cannot be punished twice for the same offence."

[67] Article 15 of the Regulation (EU) 2023/154.

Rights of the person whose data is sought

An individual whose data is sought has a limited number of rights under the e-Evidence package. For example, the person whose data is being requested has the right to be informed of the production of data by the issuing authority unless a reason for delaying or restricting the information applies on the part of the issuing authority[68]

The Regulation also notes that an individual has the right to effective remedies against the order before a court in the issuing State.[69] Commentators have noted that the right to an effective remedy could be problematic if the affected person does not reside in the country and/or has little knowledge of the legal system of the issuing member state.[70]

Summary of procedure for issuing and enforcing European Production and Preservation Orders

As mentioned above, the EU e-Evidence Package consists of two instruments – a Regulation which will apply from 18 August 2026 and a Directive, which was required to be transposed into Irish law by 18 February 2026. The Directive requires Member States to develop rules for certain service providers to appoint legal representatives for the purpose of gathering electronic evidence in criminal proceedings.

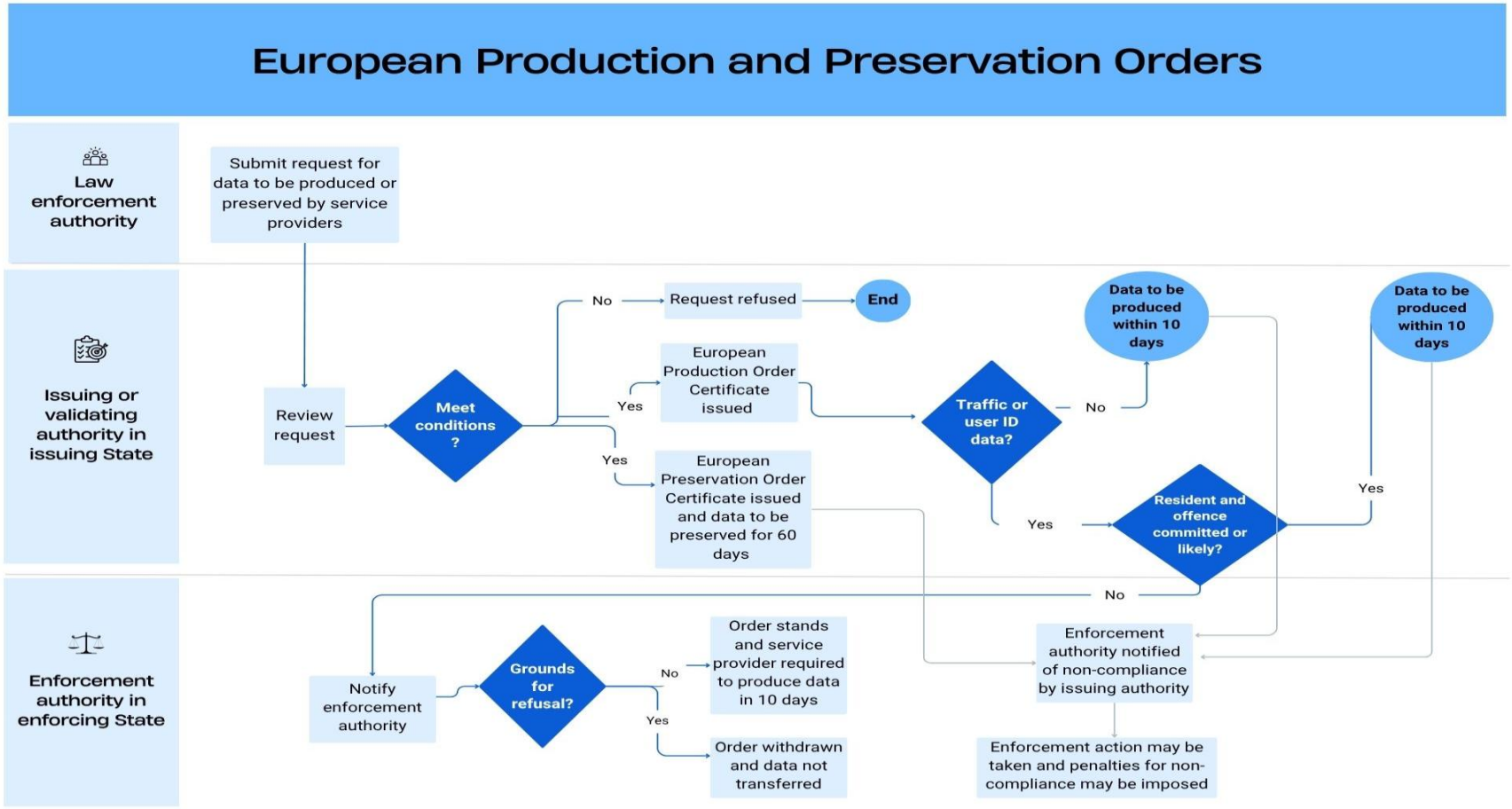
The Regulation allows for law enforcement authorities in one EU Member State to request electronic data from service providers in another EU Member State. These requests are processed by the issuing authority in the Member State where the request originates. The Regulation also requires an enforcement authority in the other Member State to ensure compliance with these orders and it may also refuse certain European Production Orders in certain circumstances. The process is set out in summary form in the infographic on the next page.

---

[68] Article 13 of the Regulation (EU) 2023/154.

[69] Article 18 of the Regulation (EU) 2023/154.

[70] Christakis, T. (2025) 'From Mutual Trust to the Gordian Knot of Notifications: The EU e-Evidence Regulation and Directive', in V. Franssen and S. Tosza (eds.) *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge: Cambridge University Press (Cambridge Law Handbooks), pp 173–199.



Source: PRS (2026), based on Regulation (EU) 2023/1543

Related EU instruments

In its Impact Assessment of the e-Evidence package, the European Commission noted:

> *... there are many co-existing levels of regulation: EU law, rules at Member State level governing criminal investigations, international conventions and bilateral agreements. US law also plays an important role, as major service providers holding relevant evidence operate under US jurisdiction.*

It also recognised that:

> *Some aspects of the legal environment are currently subject to changes:*
>
> *• several EU instruments are currently under revision, such as the ePrivacy Directive, and new proposals are being prepared;*
>
> *• work has recently started on an additional protocol to the Council of Europe Budapest Convention on Cybercrime, the main international framework governing access to electronic evidence by public authorities;*
>
> *• like the EU and its Member States, the US is trying to address the issues created by cross-border access to e-Evidence through legislative initiatives.*[71]

Therefore, the purpose of this section is to provide an overview of related EU and international instruments. This will illustrate the impact that the EU E-Evidence package has on other areas of digital regulation.

European Investigation Order

The European Investigation Order (EIO) is a judicial decision issued in or validated by the judicial authority in one EU country to have investigative measures to gather or use evidence in criminal matters carried out in another EU country. This instrument is based on mutual recognition and provides a range of investigative measures including, the hearing of witnesses, telephone interceptions, covert investigations and information on banking operations.

The EIO was established by EU Directive 2014/41/EU and applied throughout the EU except in Denmark and Ireland. In 2010, Ireland chose not to opt into the draft European Investigation Order (EIO) proposal "on the basis that it was inconsistent with Irish law and practice"[72].

---

[71] Under the Treaty of Lisbon, Ireland and the United Kingdom (UK) negotiated Protocol No. 21 ("Protocol 21") to the Treaty on the Functioning of Europe (TFEU) which excluded them from automatic participation in measures related to the area of freedom, security and justice' (Title V of Part Three of the TFEU).

[72] EU Directives – Wednesday, 4 Jun 2014 – Parliamentary Questions (31st Dáil) – Houses of the Oireachtas.

Therefore, the current practice is that if a request for the execution of a European Investigation Order is received by Ireland it will be kept on hold until the request is either withdrawn or submitted as a standard mutual legal assistance request. [73]

The Minister for Justice, Home Affairs and Migration, Jim O'Callaghan TD stated he has received agreement in principle from Government to opt in to the European Investigation Order Directive.[74] The Houses of the Oireachtas will, however, have to pass a motion to opt-in to this measure. The European Investigations Order Bill was listed on the 'All Other Legislation' section of the Summer Legislation Programme 2026.

In its 2025 Policy Priorities document, Technology Ireland called for Ireland to opt into the Directive in advance of February 2026 to "avoid service providers headquartered in Ireland being required to designate an establishment or legal representative in another EU Member State to receive and process EIOs."[75]

Data Retention

In 2014 the Court of Justice of the European Union (CJEU) declared the Data Retention Directive[76] to be invalid on the grounds of a serious interference with fundamental rights and a lack of specific access safeguards.[77]

In May 2025, the European Commission launched a call for evidence for an impact assessment on data retention by service providers for criminal proceedings.[78] The Commission has indicated on its website that it will now "consider and assess different options, both non-regulatory and regulatory measures". The Programme for Government contains a commitment to "work with EU colleagues to enact an EU Wide Data Retention law".[79]

---

[73] According to information on Mutual Legal Assistance available on: gov.ie

[74] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. See also: Strengthening Justice in the Digital Age: Ireland's Leadership under the EU e-Evidence Regulation.

[75] Technology Ireland (IBEC) Unlocking the Future Technology Ireland Policy Priorities 2025.

[76] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

[77] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others.* See CJEU (2014) The Court of Justice declares the Data Retention Directive to be invalid, press release.

[78] European Commission (2025) Call for evidence for an impact assessment on retention of data by service providers for criminal proceedings - Ares(2025)4081079.

[79] Government of Ireland (2025) Programme for Government 2025 Securing Ireland's Future, p 121.

Reflecting on the intersection between data retention and the EU e-Evidence package, the European Union Agency for Criminal Justice Cooperation (Eurojust) and the European Judicial Cybercrime Network (EJCN) conclude:

> *The e-Evidence package has introduced new tools and mechanisms that aim at strengthening international cooperation. A minimum level of certainty and uniformity with regard to the availability of data is, however, required for these tools and mechanisms, and by extension, international cooperation, to be effective. In this context, providing for adequate minimum data retention periods would ensure sufficient time to enable effective criminal investigations.*[80]

This view is reinforced by the High-Level Group on access to data for effective law enforcement, which recommends that the development of "a harmonised EU framework regulating the retention of metadata for law enforcement purposes is needed".[81] The Group notes that "by ensuring that data is retained, such a framework would support the full implementation of the e-Evidence package". In particular the High-Level Group states:

> *Exploiting synergies with the e-Evidence package would save costs and resources and contribute to the full implementation of the e-Evidence legislation. For example, encouraging [law enforcement authorities] LEAs to create or expand the capacity of units acting as SPoC*[82]*s for (cross-border) data disclosure requests could be extended to requests made at national level, or the requirement to provide training programmes for investigators and first responders. Equally, the efforts currently ongoing in the context of the implementation of the e-Evidence package to set up a digital platform to allow for direct exchanges between competent authorities and providers could be replicated for the purpose of communication metadata retained based on national legislation.*[83]

---

[80] European Union Agency for Criminal Justice Cooperation (Eurojust) and the European Judicial Cybercrime Network (EJCN) (2024) *The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU*, p 20. This report was based on the responses to a questionnaire provided by all 27 Member State representatives of the European Judicial Cybercrime Network (EJCN), and provides an overview of the legal developments concerning data retention in the EU as well as a practitioner-based assessment of the impact of the case-law from the Court of Justice of the European Union (CJEU) on the collection of evidence and judicial cooperation in criminal matters.

[81] *Concluding report of the High-Level Group on access to data for effective law enforcement*, 15 November 2024, p. 33.

[82] This refers to designated single points of contact within platforms.

[83] *Concluding report of the High-Level Group on access to data for effective law enforcement*, 15 November 2024, p 32.

Lawful Interception

In its Concluding Report, the High-Level Group on access to data for effective law enforcement recommended:

> *devising an EU instrument on lawful interception (consisting of soft-law or binding legal instruments) for law enforcement purposes that would establish enforceable obligations for providers of [electronic communications services] ECS in the EU.*[84]

In developing such instruments, the Group recommended that "inspiration" should be drawn "from the work done in the context of the adoption of e-Evidence rules".[85]

In January 2026, the Minister for Justice, Home Affairs and Migration, Jim O'Callaghan TD, announced he had secured government approval for the development of a Communications (Interception and Lawful Access) Bill. In this press release, the Minister noted the alignment of this Bill with a number of policy and legal instruments related to the EU e-Evidence package, namely the EU Commission's "*Roadmap for lawful and effective access to data for law enforcement*"; the Council of Europe Convention on Cybercrime (Budapest Convention) and the European Convention on Mutual Assistance.

Related international instruments

In a 2025 speech by Minister for Justice, Home Affairs and Migration, Jim O'Callaghan TD, stated:

> *The implementation of e-Evidence package is taking into consideration of other international instruments such as the UN Convention against Cybercrime, and the Council of Europe Budapest Convention.*[86]

This section of the Paper will provide an overview of the contents of some of those instruments.

Council of Europe Convention on Cybercrime (Budapest Convention)

Ireland signed the Council of Europe Convention on Cybercrime on 28 February 2002 but has not yet ratified it. The Budapest Convention provides for:

---

[84] *Concluding report of the High-Level Group on access to data for effective law enforcement*, 15 November 2024, p 48.
[85] *Concluding report of the High-Level Group on access to data for effective law enforcement*, 15 November 2024, p 48.
[86] Strengthening Justice in the Digital Age: Ireland's Leadership under the EU e-Evidence Regulation.

(i) the criminalisation of conduct – ranging from illegal access, data and systems interference to computer-related fraud and child pornography;

(ii) procedural powers to investigate cybercrime and secure electronic evidence in relation to any crime; and

(iii) efficient international co-operation.[87]

The Criminal Justice (Offences Relating to Information Systems) Act 2017 gave effect to some of the substantive offences in the Convention, but the procedural provisions have not yet been provided for in Irish law. It is expected that this will be given effect by the Criminal Justice (Protection, Preservation of and Access to Data) Bill, as provided for in Part 2 of the General Scheme.

Council of Europe's Third Additional Protocol to the European Convention on Mutual Legal Assistance in Criminal Matters

The Third Additional Protocol was adopted by the Council of Europe's European Committee on Crime Problems on 04 June 2025 and it was opened for signature and ratification on 9 September 2025. According to the Council of Europe's press release:

> *The new Protocol aims to strengthen the capacity of member and partner states to respond effectively to crime, particularly in a context of rapid political, social and technological change. The main advances include:*
>
> - *simplification and acceleration of mutual assistance procedures ;*
> - *extending the range of situations in which mutual assistance may be requested;*
> - *broadening the use of electronic communication channels and video conferencing; enabling the use of technical surveillance tools such as GPS trackers and telecommunications interception; and introducing time limits.*

On 10 December 2025, Dáil Éireann passed a motion to opt-in[88] to a European Commission Proposal for a Council Decision authorising Member States to sign, in the interest of the European Union, the Third Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters.

---

[87] Council of Europe (2025) Joining the Convention on Cybercrime: Benefits.

[88] Ireland exercised this "opt-in" under Protocol No. 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union.

United Nations Convention against Cybercrime

The United Nations Convention against Cybercrime was adopted by the General Assembly of the United Nations on 24 December 2024 in New York by resolution 79/243. The Convention is comprised of nine chapters, two of which are relevant to this paper and provide for the following, among other matters:

- **Procedural measures and law enforcement**: Such as expedited preservation, search and seizure of stored electronic data, production orders for electronic data or subscriber information, and the interception of traffic or content data in transit.
- **International cooperation**: This enables States parties to request other parties to preserve electronic evidence, access data or intercept traffic or content data.

Ireland signed the Convention on 25 October 2025 but has not yet ratified it.

US CLOUD Act

On 23 March 2018, the U.S. Congress adopted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), to improve procedures for both the United States and foreign authorities in obtaining access to data held by online service providers for the purposes of criminal investigations. This legislation was introduced following the *Microsoft Ireland* litigation, which considered whether a United States court could require the production of data held in Ireland.[89] According to EUROJUST, some challenges remain in terms of enforcement issues and conflicting legal obligations for the service providers.[90]

[89] For further discussion see: Jennifer Daskal, 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0' (2018) 71 *Stanford Law Review Online* 9.

[90] EUROJUST (2022), The CLOUD Act.

Potential implications of legislative proposals

As mentioned earlier in this Paper, the Government intends to bring forward legislation to give effect to the EU e-Evidence package and other mutual legal assistance instruments.

The General Scheme of the Criminal Justice (Protection, Preservation of and Access to Data) Bill was published on 8 February 2024. The Joint Oireachtas Committee on Justice, Home Affairs and Migration concluded pre-legislative scrutiny on 5 March 2024, following an oral briefing from Department officials on that date. The General Scheme is comprised of 13 Heads which are divided into four Parts as follows:

- Part 1 – General
- Part 2 – Budapest Convention
- Part 3 – European Preservation and Production Orders
- Part 4 – Terrorist Content Online

It should be noted that Part 4 of the General Scheme does not relate to cooperation on electronic evidence in criminal proceedings but rather relates to the EU Terrorist Content Online Regulation, which will be discussed in more detail in the forthcoming *Bill Digest.*

The General Scheme of the Criminal Justice (International Cooperation Office) Bill was published on 3 June 2025. The General Scheme is comprised of 19 Heads which are divided into four Parts as follows:

- Part 1 – Preliminary and General
- Part 2 – Office for Criminal Justice International Cooperation
- Part 3 – Obligation of Service Providers under the Electronic Evidence Directive
- Part 4 – Sanctions under the Electronic Evidence Directive and EPO Regulation

The Joint Oireachtas Committee on Justice, Home Affairs and Migration published its Report on Pre-Legislative Scrutiny of the General Scheme of the Criminal Justice International Cooperation Office Bill 2025 on 17 December 2025. The Committee received a briefing from Department officials on 9 December 2025 as part of the pre-legislative scrutiny process and indicated its preference was to conduct further hearings but had to conclude its scrutiny due to the Minister's intention to publish the Bill in early 2026.

As previously noted, the Minister for Justice, Home Affairs and Migration, Jim O'Callaghan TD received agreement in principle from Government to opt in to the European Investigation Order Directive.[91] The Houses of the Oireachtas will, however, have to pass a motion to opt-in to this measure. The European Investigations Order Bill was listed on the 'All Other Legislation' section of the Summer Legislation Programme 2026.

This section of the *Paper* will trace potential implications of these legislative proposals from a thematic perspective.

---

[91] Strengthening Justice in the Digital Age: Ireland's Leadership under the EU e-Evidence Regulation.

Proposed new Office for Criminal Justice International Cooperation (CJICO)

As outlined above, Part 2 of the General Scheme of the Criminal Justice (International Cooperation Office) Bill provides for the establishment of a new criminal justice agency, the Office for Criminal Justice International Cooperation. The Minister for Justice, Home Affairs and Migration, Jim O'Callaghan TD, in a 2025 speech stated the proposed new International Cooperation Office:

> *... will be a central hub for digital and judicial cooperation and will bring coherence, efficiency, and expertise to Ireland's international digital cooperation in criminal justice.*[92]

The General Scheme proposes to designate the Director of this Office as the 'enforcement authority' for the purposes of the e-Evidence Regulation. The Director will also be designated the 'central authority' under the Regulation and the e-Evidence Directive.[93] The General Scheme also provides that the Minister may designate the Director as "the responsible authority for other functions in facilitating criminal justice cooperation with other states".[94] Commenting on the future of the office, the Minister noted:

> *... in addition to roles under the EU e-Evidence package its anticipated that the office could take on additional roles in the Criminal Justice International Cooperation sphere in the future. This may include functions related to terrorist content online regulation, European investigation orders, should we opt in, mutual legal assistance, European arrest warrants, domestic production and investigation orders and indeed the EU US Cloud Act Agreement.*[95]

The Regulatory Impact Assessment for the General Scheme noted that the Department of Justice undertook a stakeholder engagement exercise in its consideration of regulatory model options. These options included assigning regulatory roles to existing functions or agencies within the Department of Justice and the designation of regulatory bodies outside the criminal justice sector, such as the Commission for Communications Regulation (telecommunications service providers) 'COMREG' and Coimisiún na Meán. Having considered these options the Department favoured the establishment of a single regulatory body which would align with the "EU Commission's recommendation that EU Member States create more central and specialised units that would more effectively contribute to international judicial cooperation."[96] The Department then considered two options as follows:

- Option A: To provide for the appointment of an office holder, who would be appointed for a fixed term (renewable) and be resourced by the Department (finance, staff, office space, etc).

---

[92] Strengthening Justice in the Digital Age: Ireland's Leadership under the EU e-Evidence Regulation.

[93] Head 2.3 (1) of the General Scheme of the Criminal Justice (International Cooperation Office) Bill.

[94] Head 2.3(5) of the General Scheme of the Criminal Justice (International Cooperation Office) Bill.

[95] Strengthening Justice in the Digital Age: Ireland's Leadership under the EU e-Evidence Regulation

[96] Regulatory Impact Assessment EU e-Evidence Package, p 7.

- Option B: To provide for the creation of a new stand-alone body, with its own budget/vote, governance arrangements (Board, Chief Executive Officer, corporate plan, accountability to PAC and Oireachtas Committees, role of Minister in giving policy directions, etc) and power to acquire office space and recruit staff.

The Department recommended option A as the most cost-effective model and noted that:

> *An office-holder model, as opposed to a stand-alone body model, allows for flexibility and celerity, in that it would efficiently grant the necessary level of independent decision making and function delegation, while also maintaining linkages and a relationship with the Minister(s), Government and the Oireachtas.*[97]

In a briefing to the Joint Oireachtas Committee on Justice, Home Affairs and Migration, Departmental officials noted that "a significant number of the largest social media and electronic communications service providers have their European presence in Ireland" and therefore, "a conservative estimate is that Ireland will receive in excess of 300,000 orders per annum".[98]

In its Report on pre-Legislative Scrutiny of the General Scheme of the Criminal Justice International Cooperation Office Bill 2025, the Joint Oireachtas Committee on Justice, Home Affairs and Migration expressed concerns about:

- The lack of clarity around the staff of the proposed office and whether they will be required to have relevant legal expertise and experience;
- The ability to process a potential 300,000 cases per year (or 1,000 per day);
- Whether a budget of €2.8 million and 30 staff will be sufficient in terms of resourcing, and whether this will negatively impact existing staff levels within the Department of Justice;
- The lack of clarity and oversight regarding the role of the proposed office in reviewing data prior to its transfer;
- Whether AI will be used to process applications; and
- The lack of transparency as to how the State and providers will handle requests for data.

In the recruitment advertisement for the Director of the CJICO, it is stated that "at full operation from 2028, it is anticipated that the office will comprise 150 staff working across its [four] divisions".

---

[97] Department of Justice (2025) Regulatory Impact Assessment EU e-Evidence Package, p 9.

[98] Joint Oireachtas Committee on Justice, Home Affairs and Migration(2025) Report on pre-Legislative Scrutiny of the General Scheme of the Criminal Justice International Cooperation Office Bill 2025, p 6.

Fundamental rights concerns

A European Commission official has noted that:

> *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.*[99]

These States were Germany, Croatia, Hungary, Poland, and Finland. Much of the criticism related to the grounds for refusal with Germany, Hungary and Poland's concerns related to the ground for refusal in case of a manifest breach of a fundamental right. Voting against the adoption of the Regulation, Finland called for the inclusion of a ground restricting production orders for traffic and content data to certain offences or to offences punishable by a certain minimum threshold. Finland also argued that a judicial assessment should also be carried out in the enforcing State in relation to the most sensitive data.[100]

The e-Evidence package has also been criticised by academics for its "minimal fundamental rights safeguards".[101] For example, Shurson notes that while the grounds for refusing a European Investigation Order included "incompatibility with fundamental rights", the e-Evidence Regulation requires a higher threshold of refusal which is limited to 'a manifest breach' of a fundamental right.[102]

In its Report on pre-Legislative Scrutiny of the General Scheme of the Criminal Justice International Cooperation Office Bill 2025, the Joint Oireachtas Committee on Justice, Home Affairs and Migration raised a number of concerns, including fundamental rights issues, about the operation of the new system as follows:

- The possibility of double-criminality, and whether Ireland will inadvertently contribute to poor human rights practices;
- Whether Ireland will be facilitating the prosecution of individuals who have committed an act or acts that here would not constitute a criminal offence;
- The requirement for a publicly accessible register, providing information on requests received from other member states, how those requests are processed and their respective outcomes;

---

[99] Juszczak (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, *EU Crim,* Issue 2/2023, pp 182-200, at 200.

[100] Ibid.

[101] Shurson (2025) 'The Balance of Efficiency and Fundamental Rights in the EU E-Evidence Regulation', *New Journal of European Criminal Law,* Volume 16 Issue 3, pp 278-299.

[102] Ibid.

- The lack of safeguards and incentives for providers to consider data protection rights and fundamental rights.[103]

In its submission to the Joint Oireachtas Committee on Justice, Home Affairs and Migration, Digital Rights Ireland suggests two recommendations to promote fundamental rights, namely:

- An amendment to the penalties provision (in Head 4.4 of the General Scheme of the Criminal Justice (International Cooperation Office) Bill) to include a provision mitigating penalties where a provider has acted in good faith to safeguard the rights of their users or affected third parties, and
- Inclusion of a notification requirement (in Head 5 of the General Scheme of the Criminal Justice (International Cooperation Office) Bill) requiring service providers to notify individuals whose data has been accessed, unless the issuing authority has asserted one of the exceptions to mandatory notification in the European Production Order Certificate.[104]

Implications for the Judicial and Law Enforcement Authorities

In its Pre-Legislative Scrutiny of the General Scheme of the Criminal Justice International Cooperation Office Bill 2025, the Joint Oireachtas Committee on Justice, Home Affairs and Migration expressed concerns about additional pressure on the courts. In response, the Courts Service noted:

> *Discussions with the Department of Justice, Home Affairs and Migration (DJ HAM) suggest that the volume of cases is expected to be low, as service providers are not anticipated to challenge decisions of the Criminal International Cooperation Office on a large scale. This expectation appears to be informed by DJHAM's consultations with service providers and previous experience in similar contexts where data was sought. That said, the Courts Service acknowledges that this projection may prove optimistic, and the situation may need to be reviewed post -commencement.*[105]

The Courts Service made the following observations on the General Scheme:

- some appeals cases may be complex and could require significant court time, particularly where penalties involve substantial sums of money (Head 4.7)
- requiring a Court to confirm an uncontested decision by a new agency may not be the most efficient use of resources (Head 4.8)
- it is difficult to quantify the potential impact of the prosecution of new offences on the criminal courts.

---

[103] Joint Oireachtas Committee on Justice, Home Affairs and Migration, (2025) Report on pre-Legislative Scrutiny of the General Scheme of the Criminal Justice International Cooperation Office Bill 2025, pp 1-2.

[104] Ibid, pp 10-12.

[105] Ibid, p 53.

The Courts Service also noted the broader implications of the e-Evidence package in the context of developments in related areas of law:

> *... I have concerns about the impact of the broader legislative programme in addressing data issues and also the outcome of the decision of the European Court in the Dwyer case. In its view, the central role that Courts are to play in managing applications relating to data access will need careful planning and resourcing if it is not to impact on other areas of Court activity.*
>
> *Data related proceedings are and will continue to grow with the commencement of this Scheme, the 2024 Bill, planned new regulations to support the Irish Passenger Information Unit and also the Communication (Retention of Data) (Amendment) Act 2022 which is already operational.*[106]

In a survey of judicial practitioners across the EU, the following implications of the e-Evidence package were anticipated:

> *Clear deadlines for service providers to respond to these orders are anticipated to significantly improve the timeliness of obtaining electronic evidence, including in urgent cases. Additionally, the EU Electronic Evidence Directive mandates that service providers offering services in the EU have an establishment or representative within the EU, regardless of their location. This requirement is expected to facilitate the appropriate direction of European Production Orders and European Preservation Orders to service providers, thereby expediting the process and reducing jurisdictional complexities that often delay MLA and EIO processes.*[107]

The SIRIUS report also surveyed law enforcement authorities who reported that the e-Evidence package would make it faster to obtain electronic evidence from service providers. Some officers also highlighted that the new system may mean that service providers may no longer disclose data voluntarily, given the focus on complying with the measures in the e-Evidence package. Others reported that "there may be issues with the detection and prevention of incidents where no criminal pre-trial investigation is yet existing".[108] This report also highlighted low levels of awareness and familiarity with the EU e-Evidence package, which indicates that training will be required to ensure that law enforcement authorities are familiar with new procedures.[109]

---

[106] Joint Oireachtas Committee on Justice, Home Affairs and Migration, (2025) Report on pre-Legislative Scrutiny of the General Scheme of the Criminal Justice International Cooperation Office Bill 2025, pp 10-12 and 52.

[107] European Union Agency for Law Enforcement Cooperation and European Union Agency for Criminal Justice Cooperation (2024) 6th Annual SIRIUS EU Electronic Evidence Situation Report, p 28.

[108] Ibid, p 28.

[109] Ibid, p 27.

Implications for service providers

Service providers will be subject to a range of obligations as outlined earlier in this paper. In a 2025 speech, the Minister for Justice, Home Affairs and Migration, Jim O'Callaghan TD, stated:

> *It is expected that over 600 service providers could designate their 'addressee' in the State, and it's estimated that the number of production orders issued to those service providers will be in the hundreds of thousands annually.*[110]

The Department's SME Test noted, however, that SMEs are "anticipated to receive a very small proportion of requests to produce digital evidence".[111] In the Department's Small and Medium Enterprise (SME) Test it is "estimated that five large service providers currently receive 95% of all current cross-border requests in Europe."[112]

The service providers who were interviewed for the SIRIUS Report 2025 gave the following view on the forthcoming EU e-Evidence legislative package:

> *Some providers feel comfortable with the new rules, are ready to implement them, and do not expect the Electronic Evidence legislative package to significantly alter their operating procedures. Others have started adapting their processes to the new rules, whereas a smaller group is waiting for full clarity before taking any action.*[113]

Providers interviewed for the SIRIUS Report also shared a number of concerns, expectations, and potential future challenges, which may be summarised as follows:

- Providers agree on the need for a large multi-stakeholder effort in order to prepare for the implementation of the EU Electronic Evidence legislative package in a smooth, efficient and homogeneous manner.
- The anticipated increase in the volume of orders that providers will have to handle also emerged as an element of concern.
- The decentralised IT system for secure digital communication and data exchange between competent authorities and service providers remains a topic of high concern. Particular concerns relate to compatibility with internal systems as well as confidentiality and security of data.
- Cooperation with single points of contact.
- Providers reported that their decision on whether forms of voluntary cooperation will be maintained after August 2026 largely depends on the correct interpretation and application of the new rules.[114]

---

[110] Strengthening Justice in the Digital Age: Ireland's Leadership under the EU e-Evidence Regulation

[111] Department of Justice (2025) SME Test EU e-Evidence Package, p 3.

[112] Ibid, p 3.

[113] European Union Agency for Law Enforcement Cooperation and European Union Agency for Criminal Justice Cooperation (2024) 6th Annual SIRIUS EU Electronic Evidence Situation Report, p 62.

[114] Ibid, p 63.

In its Budget 2026 Submission, Technology Ireland[115] called for "adequate and flexible funding for the establishment of the Criminal Justice International Cooperation Office". The lobby group also stated:

> *To meet increasing demand and respond to unforeseen needs, we request sufficient core funding to maintain essential service levels and continuity along with the ability to scale services up in response to demand surges or emergencies.*[116]

[115] Technology Ireland (IBEC) is an association with over 270 member companies, with over 100 of those being indigenous Irish technology companies. See Technology Ireland (IBEC) Unlocking the Future Technology Ireland Policy Priorities 2025.

[116] Technology Ireland (IBEC), *Budget Submission 2026*, p 11.

Conclusion

Electronic data is increasingly relied upon in the investigation and prosecution of crime. Given the transnational nature of electronic data, law enforcement authorities rely on international cooperation to access such data. Traditional methods of mutual legal assistance, which relies primarily on court-based procedures, have proved ineffective in acquiring electronic data. This area of law lies at the intersection of criminal procedure and the law of evidence and is shaped by domestic, EU and international law, including the Budapest Convention and UN Convention against Cybercrime.

The EU e-Evidence package (consisting of two instruments: Regulation (EU) 2023/1543 and Directive (EU) 2023/1544) was developed to speed up access to data by providing for European Production Orders and European Preservation Orders. The Criminal Justice (Protection, Preservation of and Access to Data) Bill proposes to give judicial authorities in Ireland the power to issue these orders. Member States are required to designate enforcement authorities to ensure compliance with these orders. To that end Ireland is proposing to establish a new body, the Criminal Justice International Cooperation Office (CJICO), via the Criminal Justice (International Cooperation Office) Bill, which will have a range of enforcement powers including the imposition of penalties of up to 2 per cent of the service provider's total worldwide annual turnover in the preceding financial year.

During pre-legislative scrutiny, the Joint Oireachtas Committee on Justice, Home Affairs and Migration raised concerns about the financial and human resources dedicated to the CJICO, which will have a staff of 150 by 2028. Given the number of digital service providers with European headquarters located in Ireland, it is anticipated that service providers based in Ireland will receive in excess of 300,000 orders per annum.

The Joint Oireachtas Committee on Justice, Home Affairs and Migration also raised a number of other concerns, including a lack of safeguards and incentives for service providers to consider data protection rights and fundamental rights as well as a lack of transparency as to how the State and providers will handle requests for data. The Government has stated that successful implementation of the package will have "a major strategic impact on Ireland's reputation as a hub for digital regulation, and on its ability to ensure effective access to digital evidence in tackling serious crime".[117]

It is likely that the implementation of the EU e-Evidence package will lead to Ireland opting into other EU instruments in this field, such as the European Investigation Order Directive. Ireland is also likely to contribute to forthcoming EU proposals on data retention and lawful interception. This may in turn lead to an expansion of the remit of the CJICO.

---

[117] Recruitment advertisement for the Director of the Criminal Justice International Cooperation Office.