

e-Evidence Package: Increased obligations on service providers to cooperate with data requests from law enforcement authorities

19 November 2024

This article, relating to EU law, was written by the team in our Dublin office for Browne Jacobson Ireland LLP.

A new legislative package is set to take effect in 2026, consisting of Regulation (EU) 2023/1543 (the Regulation) and Directive EU 2023/1544 (the Directive), in relation to the gathering of electronic evidence (together the e-Evidence Package).

Although the new regime operates within the confines of criminal proceedings, companies, particularly service providers, should be aware of the obligations that can be imposed on them under this regime.

Electronic evidence such as text messages and emails are becoming increasingly integral to criminal investigations. As it is no longer necessary to rely upon physical infrastructure for data storage, data is being stored in a more fragmented and often temporary manner. Accordingly, it is becoming progressively common for data to be stored outside an investigating state or by an international service provider. The European Commission estimates that nowadays more than half of all criminal investigations include a cross-border request to access electronic evidence from another EU member state. These cross-border requests can present significant challenges for the law enforcement and judicial authorities involved in the gathering of electronic evidence, particularly given the often-volatile nature of electronic evidence.

Currently, multiple international cooperation instruments exist within the EU to facilitate cross-border electronic evidence requests. In Ireland, the Mutual Legal Assistance Convention (MLAC), is given effect by the Criminal Justice Mutual Assistance Act 2008 (as amended), which currently governs any such cross-border requests in relation to criminal proceedings made by law enforcement and judicial authorities between Ireland and other EU Member States. The current regimes are increasingly becoming associated with long wait times and often law enforcement authorities opt to instead rely on ad-hoc informal requests, along with the good faith cooperation of service providers.

The e-Evidence package seeks to streamline the current regime in offering an alternative mechanism. It will also assist in creating a more harmonised system and in maintaining the integrity of any such electronic evidence.

Who will be impacted by the e-Evidence Package?

The Regulation applies to a broad range of service providers who offer services in the EU, regardless of their place of establishment.

‘Service provider’, means any natural or legal person who provides one or more of the following categories of services:

- Electronic communications;
- Internet domain name and IP numbering services;
- Other information society services which enable users to communicate with one another or enable the processing and storage of data, where storage is a defining component of the service provided.

This third category of services is particularly far reaching insofar as capturing a large number of distant Service Providers e.g., those who may facilitate chat or comment functions ancillary to their main service, other hosting services including where the service is provided via

cloud computing, online gambling and gaming platforms.

Introduction of a European Production Order and European Preservation Order

The Regulation will introduce both a new European Production Order for Electronic Communications (EPOC) and a European Preservation Order for Electronic Communications (EPOC-PR).

The EPOC will facilitate a judicial authority in one EU state to obtain electronic evidence directly from a service provider, or its legal representative, in another EU state. The service provider will be obliged to respond within 10 days, or within eight hours for emergency cases. This contrasts with the current average time limit of 10 months associated with the MLAC.

Separately the EPOC-PR will allow a judicial authority in one EU country to request that a service provider, or its legal representative, in another EU country preserves specific data in view of a subsequent request to produce this data via either the existing MLAC regime, a EPOC or EPOC-PR.

Service providers will be able to seek clarification on any orders which they believe are incomplete or which contain any errors. There will also be two legal grounds available for service providers to raise in refusal of a request, namely, immunities / privileges or conflicts with any obligation under the applicable law. Additionally, a request can be refused on the basis of impossibility where a service provider informs the issuing authority, explains to it the basis for asserting impossibility, and where the authority confirms such impossibility exists.

Designation of establishment or appointment of a legal representative

The Directive will require any service providers offering services in the EU to designate an establishment or appoint a legal representative within the EU who will be charged with receiving and complying with any cross-border requests. A legal representative will need to be appointed as an addressee where a service provider is not established in the State but offers services in the EU. A legal representative can be any natural or legal person. Both designated establishments and legal representatives should be equipped with the necessary powers and resources in order to comply with any such requests.

The Directive will require transposition by Member States by the 18 February 2026 and correspondingly, the obligation to designate an establishment or appoint a legal representative will need to be carried out by the same date. If a service provider begins offering services after this date, they will have six months from this date to designate an establishment or appoint a legal representative. Separately, the Regulation will apply from the 18 August 2026.

In Ireland, the Criminal Justice (Protection, Preservation and Access to Data on Information Systems) Bill 2024 will seek to give effect to the provisions of the e-Evidence Package, this is currently at pre-legislative scrutiny stage.

Distinction from the preclusion of general and indiscriminate retention of data

The EPOC and EPOC-PR to be introduced will involve requests for data stored by a service provider at the time of receipt of the relevant order only. In other words, the Regulation will not impose a general retention obligation on service providers, and it should not result in general and / or indiscriminate retention of data.

Fines for non-compliance

There will be significant penalties associated with infringement with potential fines of up to 2% of the total worldwide annual turnover of the preceding financial year of the associated service provider. These fines can arise in circumstances where the service provider without accepted refusal, fails in their obligations to:

- provide the requested data;
- provide the exhaustive data requested;
- provide the data in line within the relevant deadline or extended deadline;
- preserve the data requested; and / or

- implement the associated operational and technical measures to ensure confidentiality, secrecy and integrity of the associated data.

In calculating fines, all relevant circumstances will be considered e.g., gravity and duration of any breach, intentionality, financial strength of the service provider, and / or any previous breaches.

Conclusion

Companies should begin to examine whether they fall within the ambit of the e-Evidence legislative package. It is important that service providers are aware of their upcoming obligations and begin to put preparatory procedures and resources in place so that they are in a position to comply with any such evidence requests, within the strict time limits that will be required under the e-Evidence package, should they arise.

In parallel with GDPR obligations, service providers will also have to consider the veracity of any requests along with any confidentiality obligations surrounding the data concerned.

If you have any queries in relation to the above, please feel free to contact us.

Key contact



Darragh Killeen

Partner

darragh.killeen@brownejacobson.com

+353 1 574 3914

Related expertise

FinTech

HealthTech

InsurTech

IT service providers

Technology