The EU's E-Evidence Legal Framework:

Answers to Frequently Asked Questions

June 2026

Richard Salgado, Kenneth Propp & Mona Giacometti[1]

This document answers frequently asked questions about the European Union's E-Evidence legal framework.

I. Overview of Framework

1. ***What is the EU's E-Evidence legal framework?***

   It is a European Union legal regime governing cross-border access to electronic evidence in criminal proceedings. It consists of two interrelated legislative acts: Regulation (EU) 2023/1543, which establishes European Production Orders and European Preservation Orders, and Directive (EU) 2023/1544, which requires service providers offering services in the Union to designate legal representatives or EU establishments to receive order certifications and respond to them. There also are subsidiary Implementing Acts addressing technical specifications.

2. ***Why was this framework adopted?***

   It was adopted to make it easier for law enforcement in an EU Member State to collect electronic evidence, like email and other digital records, from service providers located in another country.

3. ***Who implements and enforces the E-Evidence legal measures?***

   Each Member State is responsible for applying the framework through its courts, investigating judges, prosecutors, and other authorities designated by national law. Member States are also responsible for establishing enforcement mechanisms and penalties for non-compliance. The framework operates through cooperation among the competent authorities of Member States.

4. ***What does the Regulation do?***

   The Regulation establishes the two primary legal instruments: the European Production Order and the European Preservation Order. Together, these orders enable competent authorities in one Member State to directly compel a covered service provider (e.g. a provider of services in the Union) in another country to preserve and disclose electronic evidence. It defines the categories of data that can be requested

[1] The views expressed here are solely those of the authors. The authors express their appreciation for comments on earlier drafts from participants in the Cross Border Data Forum.

(subscriber, identification, traffic, and content), sets out the mandatory conditions for issuing and for executing orders, establishes deadlines and due process guarantees, and requires the use of a secure decentralized IT system for cross-border communications. The technical specifications for that system are set out in a separate Implementing Regulation.

5. ***What does the Directive do?***

The Directive requires service providers offering services in the Union to designate a legal representative or a designated establishment in at least one Member State to act as a single point of contact for receiving and complying with preservation and production order certifications. It also requires providers to give that representative or establishment the authority and resources needed to comply with obligations under the E-Evidence framework.

6. ***What is the implementation timeline?***

The Regulation entered into force in August 2023, triggering certain obligations that Member States had to fulfill to create the basis for future implementation. The Regulation is scheduled to become fully applicable by August 18, 2026.

The Directive required transposition into Member State law by February 18, 2026. However, at the time of writing in summer 2026, many Member States have not yet enacted the domestic law measures required by the Directive. Without a designated establishment or a legal representative identified by the relevant service provider in accordance with domestic legislation, issuing judicial authorities may for the time being find themselves at a loss when determining to whom to address the production or preservation order.

II. SCOPE

7. ***Which services are covered by the Regulation?***

The Regulation covers electronic communications (e.g., VoIP, messaging), internet domain/IP services, telecommunications, and information society services that enable user interaction or store data.

8. ***What providers are covered by the Regulation?***

The Regulation applies to service providers to the extent that they offer covered services in the EU. A provider offers a service in the Union when users in at least one Member State can use the service and the provider has a substantial connection to the EU. A substantial connection exists where the provider has an establishment in a Member State or, absent an establishment, where the provider has a significant number of users in one or more Member States or targets activities toward one or more Member States.

9. ***Which kinds of data are covered by the Regulation?***

   It covers subscriber data, identification data (used solely to identify a user), traffic data (metadata), and content data (e.g., text, voice, video).

10. ***What kinds of data are explicitly not covered by the Regulation?***

    It does not cover data for services offered exclusively outside the Union, financial services, or the real-time interception of data.

11. ***Which authorities may issue orders under the Regulation?***

    Judges, courts, and investigating judges may issue European Production or Preservation Orders in criminal proceedings for all data types. Public prosecutors are limited to issuing European Preservation Orders for all covered types of data or European Production Orders for subscriber and identification data. For other data, the prosecutor needs validation by a judge, a court or an investigating judge.

    Other national investigative authorities may also issue orders, provided that such orders are validated, as appropriate, by a judge, court, investigating judge, or, if relevant, a prosecutor. Orders also may be issued on behalf of accused persons.

12. ***For what type of proceedings can the Regulation be used?***

    European Production Orders and European Preservation Orders may be issued only for criminal proceedings or for the execution of a custodial sentence or detention order of at least four months where the convicted person has absconded. Such orders may also be issued in proceedings relating to a criminal offence for which a legal person may be held liable or sanctioned under the law of the issuing State.

III. Operation in Practice

13. ***What types of orders are created by the Regulation?***

    There are two types: European Production Orders and European Preservation Orders. Service providers generally will receive not the underlying order itself, but a standardized certificate reflecting the existence of the order and specifying the provider's obligations. Those certificates are known as the European Production Order Certificate (EPOC) and the European Preservation Order Certificate (EPOC-PR), respectively.

14. ***What is a European Production Order?***

    A European Production Order is a judicial order that allows an authority in one Member State to obtain electronic evidence directly from a service provider established or represented in another Member State.

15. ***What is a European Preservation Order?***

A European Preservation Order is a judicial order that allows an authority in one Member State to require a service provider established or represented in another Member State to preserve specified electronic evidence for 60 days pending a production request, with a possible 30-day extension.

16. ***What are the underlying preconditions for issuance of these orders?***

    Orders must be necessary and proportionate, relate to the aforementioned criminal proceedings, and be available under the same conditions as in a similar domestic case. If the purpose of the order is to obtain traffic or content data, it may be issued only if the offense under investigation or for which the absconder has been convicted constitutes a specified offense (primarily offense against information systems) or an offense punishable in the issuing state by a custodial sentence of at least three years.

17. ***How are orders transmitted and served?***
    Order Certificates are transmitted directly to the provider's designated establishment or legal representative, using standardized forms. The orders themselves are not provided. In emergency cases where a covered provider has no designated establishment or appointed legal representative, the certificate may be addressed to any other establishment or legal representative of that provider within the EU.

18. ***What are the roles of the issuing authority and enforcing authority?***

    The issuing authority is the authority that issues the order and sends the corresponding certificate to the service provider. The enforcing authority has a more limited role. It becomes involved in specified cases involving traffic or content data, where it receives notice of the order and may object on certain grounds established by the Regulation, including in exceptional situations involving fundamental rights concerns. It also is responsible for enforcement in the event of provider non-compliance. The member state in which a provider chooses to register its establishment or to designate its legal representative becomes the enforcing authority for orders issued to that provider.

19. ***What are the Implementing Regulations?***

    The Implementing Acts are legally binding subsidiary instruments adopted by the European Commission to establish the uniform technical specifications and protocols necessary for the practical operation of the system, particularly the decentralized IT system.

IV. PROVIDER OBLIGATIONS AND COMPLIANCE STRUCTURE

20. ***What is an EU representative?***

    An EU representative is a natural or legal person designated by a service provider to act on its behalf in the Union for the receipt, compliance, and enforcement of orders

issued under the E-Evidence framework. Representatives are to have the powers and resources necessary to comply with production and preservation orders.

21. ***Why does the Regulation require that a non-EU provider that provides services within the EU designate an EU representative?***

    This requirement ensures that all providers offering services in the Union, including those based outside the EU, have at least one point of contact within the EU for receipt and enforcement of orders.

22. ***How do providers receive and respond to production and preservation orders under the E-Evidence framework?***

    Providers will utilize a decentralized IT system to receive and respond to order certifications. All written communication must eventually occur through a secure system using e-CODEX access points. e-CODEX is an existing EU system offering technical solutions for information exchange between Member States in criminal justice matters. Where communication through the decentralized IT system is not possible, an alternative may be used that is swift, secure, reliable, and sufficient to establish authenticity.

23. ***Do providers have compliance deadlines?***

    Generally, a provider must produce requested data in its possession in response to valid production order certifications within 10 days of receipt, or within 8 hours in emergency cases involving imminent threats to life, physical integrity or safety of persons or to critical infrastructure. In the case of critical infrastructure, the production is required 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 Member State.

    In cases requiring notification to an enforcing authority, the provider must produce the requested data at the end of that 10-day period (unless the enforcing authority clears it earlier). This is to ensure the enforcing Member State has the full 10 days to evaluate and potentially raise grounds for refusal before the data is disclosed. In emergency cases, the provider must transmit the data within 8 hours. The notified authority will then have 96 hours to object to the use of the data or to stipulate that it may only be used under certain conditions.

24. ***Are there grounds upon which a provider is permitted to object to orders?***

    Yes. There are procedures to object to orders that, for example, appear to be incomplete, contain manifest errors, lack sufficient information to be executed, purport to require the provider to disclose information it does not have, or that would require the provider to violate the laws of another country. Providers also may object to a timeline for response and seek an extension.

Providers typically will not receive the underlying order itself. Instead, they will receive a standardized certificate containing the information required by the Regulation, such as the issuing authority, the categories of data sought, applicable deadlines, and other prescribed details. The certificate does not require disclosure of all information underlying the order, and providers therefore may have limited visibility into factual, legal, or procedural defects that are not apparent from the face of the certificate.

25. ***What are the risks if a service provider fails to comply with orders?***

Where the service provider does not comply with an order by the deadline, without providing reasons accepted by the issuing authority, or, if notified, where the enforcing authority has not invoked any of the grounds for refusal, the issuing authority may request the enforcing authority to enforce the order.

Unless the enforcing authority considers that grounds for refusing enforcement apply, it can formally require the enforcement of the order, subject to penalties. Penalties will be determined under the national law of the enforcing Member State. These penalties should be effective, proportionate and dissuasive. They may amount to up to 2% of the service provider's total worldwide annual turnover.

In deciding the specific amount of the pecuniary penalty, the enforcing authority must take into account all relevant circumstances, including: the nature, gravity, and duration of the breach; whether the infringement was committed intentionally or through negligence; whether the service provider has been held responsible for similar previous breaches; and the financial strength of the service provider held liable. Providers must be given the right to appeal any decision to impose such a penalty.

Both the service provider and its legal representative or local establishment are subject to such penalties, under a theory of joint and several liability.

26. ***Will a provider be notified that it is covered?***

There is no mechanism through which a provider will, in advance of a legal demand for preservation or production, be notified that it is subject to the e-evidence law; as a Regulation, it is self-executing in nature.

In practice, a provider may first learn it is viewed as within scope when an EU Member State authority contacts the provider directly, including outside the EU, to say that the provider must designate a legal representative, supply contact or endpoint information, or respond to an E-Evidence order. A foreign provider with no EU establishment or legal representative might also learn of that view only when an order, preservation request, warning, or enforcement communication is sent to a publicly listed legal process address, corporate contact, registered agent, affiliate, or other known point of contact. At that point, the provider may have to assess both

whether it is covered and whether the authority has used the proper channel for service, transmission, or follow-up under the E-Evidence framework.

V. SAFEGUARDS

27. ***What judicial authorization and oversight are required?***

A European Production Order for traffic data and content must be issued or validated by a judge, a court or an investigating judge. A production order for subscriber data or data requested solely to identify a user may be issued or validated by a public prosecutor, judge, court, or investigating judge, depending on the authority designated under the law of the issuing Member State.

28. ***How are fundamental rights protections enforced?***

An enforcing authority may refuse a production order if its execution entails a "manifest breach" of fundamental rights as enshrined in the EU Charter. In that event, the issuing and enforcing authorities will undertake discussion on whether the order will be maintained, adapted or withdrawn. The provider to which the order has been directed is to be notified.

29. ***How are privileges and immunities handled?***

Orders can be refused by the enforcing authority if they interfere with immunities or privileges under the law of the enforcing State, such as attorney-client privilege, or with rules on the determination or limitation of criminal liability relating to freedom of the press or freedom of expression in other media. If the service provider believes execution could interfere with such protections, it must inform the issuing authority and, where applicable, the enforcing authority. The issuing authority shall decide whether to withdraw, adapt or maintain the order, following the consultation procedure set out in the Regulation.

30. ***Does the Regulation address the rights of persons about whom E-Evidence has been sought?***

The Regulation addresses the rights of affected persons, including rights relating to information, legal remedies, and judicial review. Whether and when a person is notified of an order is generally governed by the law of the issuing Member State. Notification may be delayed, restricted, or withheld where permitted by law, including where necessary to avoid prejudicing a criminal investigation or prosecution.

31. ***What judicial review mechanism exists for conflicts of law?***

The Regulation provides a review procedure and stipulates a comity analysis to be applied when a court must decide whether to uphold or lift an order that conflicts with third country law. The court must weigh the respective interests of the issuing

jurisdiction and the affected third country by examining a series of factors including the degree of connection for the two jurisdictions.

32. ***What legal remedies are available to those whose data is requested from a provider?***

    Any person whose data is requested has the right to effective legal remedies, which must be exercisable before a court in the issuing Member State

VI. INTERNATIONAL AGREEMENTS ON E-EVIDENCE

33. ***How does the E-Evidence Framework relate to other existing international legal mechanisms for producing evidence in criminal matters?***

    It does not affect other EU law or international agreements on the gathering of E-Evidence. These include the European Investigation Order (EIO) , the Council of Europe's Budapest Convention, and existing Mutual Legal Assistance Treaties (MLATs) maintained by the EU (such as the EU-US Mutual Legal Assistance Agreement) or by EU Member States. In theory, the E-Evidence framework should operate more quickly than MLATs because E-Evidence requests are made directly to service providers without the need for foreign government intermediation.

34. ***Does the Regulation interfere with the ability of the EU or Member States to conclude new international agreements that would operate as an exception to foreign laws that block compliance with E-Evidence requests?***

    No, the regulation does not preclude the EU or Member States from entering into E-Evidence agreements, such as one with the United States under negotiation, or mutual legal assistance treaties.

35. ***How would the E-Evidence Framework relate to the international agreement on E-Evidence under negotiation between the EU and the United States?***

    The Framework can complement an EU agreement with the United States on E-Evidence.