SQUIRE PATTON BOGGS

e-Evidence

New Cross-border Obligations for Electronic Communications Providers in the EU

EU – November 2025

As the fictional character Lester Freeman of the TV series "The Wire" put it: "We're building something, here, detective, we're building it from scratch. All the pieces matter".

Time and time again, this rings true, in every criminal investigation nowadays, where law enforcement agencies must put together key pieces of digital evidence collected across borders, including through the interception of electronic communications. Thanks to a new legal framework coming into force next year, the job of law enforcement agencies in the EU might just get a bit easier, but the burden will shift to the providers of those communications.

After five years of negotiations, the EU has adopted new legislative acts that will introduce a new system for the gathering of electronic evidence in criminal proceedings. The new rules on e-evidence consist of two legislative measures:

- Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (*O.J.* L 191, 28.7.2023, pp. 118–180)
- 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 (*O.J.* L 191, 28.7.2023, pp. 181–190)

The regulation applies from 18 August 2026. The directive must be transposed into the national laws of the EU member states by 18 February 2026.

Both acts introduce significant compliance obligations for electronic communications providers and other digital service providers operating in the EU, regardless of their place of establishment.

Key Features

1. European Production and Preservation Orders:

- Judicial authorities in one member state can issue a European Production Order (EPOC) to obtain electronic evidence (e.g. emails, messages and metadata) directly from a service provider in another member state
- A European Preservation Order (EPOC-PR) can be used to compel providers to preserve data pending a subsequent request
- Providers must respond within 10 days, or eight hours in emergency cases

2. Direct Cooperation with Foreign Authorities:

- The regulation removes the need for involvement of the service provider's home state authority, allowing direct transmission of orders across borders

3. Scope of Application:

- Applies to a wide range of providers, including electronic communications services, cloud services, social media platforms, internet domain name services and IP numbering services, as well as online marketplaces and other hosting service providers
- Even non-EU providers must comply if they target or serve users in the EU and have a substantial connection, such as local establishment or a significant user base in the EU
- The regulation applies to all companies, regardless of size, including small service providers

4. Legal Representatives and Notification Mechanisms:

- Providers must designate a legal representative or establishment in the EU to receive and respond to orders
- In certain cases, the authorities of the provider's member state may be notified and can object on limited grounds (e.g. fundamental rights, immunities or conflicts of law)

5. Decentralised IT System:

- A secure, decentralised communication platform is being developed to facilitate secure communication between authorities and service providers, as well as ensure authentication and traceability

Implications for Electronic Communications Providers

- **Compliance readiness** – Providers must establish internal procedures to process and respond to EPOCs and EPOC-PRs within tight deadlines. This includes technical capabilities, legal review processes and staff training.
- **Legal representation** – Non-EU providers targeting EU users must appoint a legal representative within the EU, creating a new layer of regulatory exposure. Our firm already serves this role of first point of contact with law enforcement agencies for several clients.
- **Data Governance and risk** – The regulation raises complex issues around data protection, conflicts of law and user notification. Providers must assess how to balance compliance with EU orders against obligations under other jurisdictions (e.g. US CLOUD Act).
- **Penalties for Non-Compliance** – Failure to comply with orders may result in significant fines based on the annual worldwide turnover, reputational damage and potential litigation.

Next Steps for Providers

- **Audit data flows** – Map where and how user data is stored and processed across jurisdictions.
- **Review contracts and policies** – Update terms of service, privacy policies and internal protocols to reflect new obligations.

- **Engage with authorities** – Monitor the development of the decentralised IT system and engage with national regulators to clarify implementation details.
- **Legal strategy** – Prepare for potential legal challenges, especially in cases involving conflicting legal obligations or sensitive data.

Additional Sector-specific Guidance

The new EU legal regime on e-evidence introduces a harmonised legal framework that affects various digital service providers differently depending on their business models, data handling practices and user base. Below is a breakdown of the implications for specific sectors:

1. Cloud Service Providers (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS))

Key Considerations:

- **Broad data scope** – Cloud providers will be required to produce not only subscriber and access data but also stored content and metadata.
- **Data localisation and segmentation** – Providers must assess how data is stored across jurisdictions, and whether it is technically feasible to isolate EU user data.
- **Encryption and access** – If data is encrypted, providers may be compelled to provide decryption keys or access credentials, raising concerns about end-to-end encryption models.

Action Points:

- Implement robust internal workflows for identifying and responding to EPOCs
- Review encryption policies and assess legal exposure related to key management
- Ensure legal representatives are trained to handle cross-border requests and escalate conflicts of law

2. Electronic Communications Services (e.g., Internet Service Providers (ISPs), Voice over Internet Protocol (VoIP) and Messaging Apps)

Key Considerations:

- **Real-time data requests** – Emergency EPOCs may require near-instantaneous access to metadata or content.
- **User notification** – The regulation limits the ability to notify users of data requests, which may conflict with transparency obligations under the General Data Protection Regulation (GDPR) or national laws.

Action Points:

- Establish 24/7 response teams to handle urgent requests
- Develop internal policies for handling user notification restrictions and documenting legal justifications
- Coordinate with data protection officers to ensure compliance with e-privacy rules

3. Social Media Platforms

Key Considerations:

- **High volume of requests** – Given their user base, platforms may face a significant number of EPOCs.
- Content moderation vs evidence preservation – Tensions may arise between removing harmful content and preserving it for legal proceedings.

Action Points:

- Automate triage systems to prioritise and route EPOCs efficiently
- Align content moderation policies with preservation obligations
- Train legal, and trust and safety teams on the nuances of the regulation

4. Online Marketplaces and Platforms

Key Considerations:

- **Transactional data** – Orders may target purchase histories, payment data or communications between buyers and sellers.
- **Third-party vendor data** – Marketplaces must determine responsibility for data held on behalf of third-party sellers.

Action Points:

- Clarify data ownership and access rights in vendor agreements
- Map data flows to ensure rapid identification of relevant information
- Prepare for potential conflicts with consumer protection or commercial confidentiality laws

5. Domain Name and IP Address Providers

Key Considerations:

- **Subscriber identification** – These providers may be required to disclose registrant data, even if minimal.
- **Data retention** – The regulation may indirectly pressure providers to retain data longer than currently required.

Action Points:

- Review data retention policies in light of potential EPOC obligations
- Ensure accurate and up-to-date registrant information is maintained
- Monitor developments in national implementation for additional obligations

Contacts

If you have any questions on any of the topics covered in this client alert, please contact any of your Squire Patton Boggs lawyers or contact the authors below:

Francesco Liberatore
Partner, Competition – Antitrust
London, Brussels and Milan
T +44 207 655 1505
E francesco.liberatore@squirepb.com

Marion Seranne
Partner, Government Investigations and White Collar
Paris
T +33 1 5383 7407
E marion.seranne@squirepb.com

The authors wish to thank Kenza Wakrim for helping with this client alert.

69764/11/25