European Commission

The EU-internal e-evidence package

HLEG 21 November 2023

Justice and Consumers

Legislative process

- Commission proposal in April 2018
- Political agreement in November 2022
- Adoption on 12 July 2023
- Entry into application: 3 years after entry into force: 18 August 2023

The package in a nutshell

- The **Regulation**: mandatory cross-border orders for the preservation and production of e-evidence directly sent to service providers offering services in the internal market; irrespective of the location of their offices, their infrastructure or the data
- The **Directive**: all service providers offering services in the Union need to designate a legal representative or a designated establishment

Scope

Which service providers are covered (Reg + Dir)?

- **Material scope**: providers of services that are used for communications purposes, the storage of data and internet infrastructure services

- **Geographical scope**: providers that are offering services in the European Union → enabling the use of services in one or more Member States and having a substantial connection to the European Union

The Directive

Obliges service providers to nominate:

- if service provider has an entity with economic activity and legal personality in the Union: a designated establishment (or several)

or

- if they have no establishment in the Union: a legal representative

→ to function as addressees of orders for the gathering of evidence

The Regulation

- Introduces new measures: a **European Production Order** and a **European Preservation Order**;
- in the framework of **criminal proceedings** (not for crime prevention) and for **execution of custodial sentences**;
- **irrespective of the data location**;
- A **certificate** is served cross-border on the representative of the service provider, with all relevant information to identify the data, but not the reasoning and details of the case.

Data covered

- Only **stored** data; no real-time interception;
- no general data retention obligations;
- **data categories**: subscriber data, data requested for sole purpose of identifying the user, traffic data, content data;
- related to the data categories (subscriber/other identification data or traffic/content data) different sets of conditions/safeguards apply.

Issuing authority

- Orders to **produce subscriber** and **other identification data** and Orders to **preserve data** (irrespective of the data category) need to be issued or validated by a prosecutor, judge or court;
- Orders to **produce traffic** and **content data** need to be issued or validated by a court or judge; not sufficient: prosecutor;
- **Ex post validation** possible in emergency cases.

Conditions for issuing an Order

- Orders to **produce subscriber** and **other identification data** as well as to **preserve** (for all data categories): all criminal offences;
- Orders to **produce traffic** and **content data**:
  - ✓ Maximum custodial sentence of at least 3 years or
  - ✓ one of the offences listed in Directives
- **Necessity** and **proportionality** requirements;
- Similar measure available under national law.

Obligations for service provider

- **Production** of the requested data within **10 days** and in **emergency cases within 8 hours**;
- **European Preservation Order:** preservation for at least 60 days or until the data is produced or declaration that it is no longer necessary;
- **Confidentiality:** no information to the person whose data is sought, nor to anybody else.
- Provisions on **enforcement** and **sanctions,** but also **cost reimbursement**

Notification regime

- Notification: of the **MS of the service provider**
- Through simultaneous transmission of certificate+
- For **traffic and content data only**
- Residence of person and offenses committed in issuing State: no notification
- **4 grounds for refusals, to be raised** within **10 days**
- Suspensive effect

Other safeguards, conditions, remedies

- All **criminal law safeguards + DP rules** apply
- **Immunities and privileges** protected
- **Comity clause** to address conflicting obligations under the rules of other countries
- **Information** and **effective remedies in issuing State** for targets
- Provider acting as **data controller,** with exceptions
- Limitations for Infrastructure provided to **privileged profession** and to **public authorities**

Decentralised IT system

- Will interconnect authorities and service providers
- In line with EU-level digitalisation efforts
- Secure communications, authentification
- Mandatory use
- Technical specifications to be developed in the next 2 years

Conclusion

- New form of judicial cooperation, more adapted to the logic of the internet
- Wide reach; departure from data storage location
- No complete departure from authority-to-authority cooperation
- Implementation challenges:
  - volume of orders
  - concentration of notifications in certain MS
  - IT system
  - Non-cooperative service providers
  - Conflicts of laws