

Internal Investigations on E-evidence: new EU-wide obligations for service providers in criminal proceedings

White Collar meets data protection law



Dr Bettina Enz



Sarah Bohn



Neil Simon-Weaver



Legal background

- Establishment of a uniform legal framework for **cross-border access to electronic evidence by law enforcement authorities** – directly from service providers, **without the need for mutual legal assistance proceedings**.
- The German Act on European Production and Preservation Orders for Electronic Evidence (“**EBewMG**”) implements the EU’s e-evidence requirements (**Directive (EU) 2023/1544** and **Regulation (EU) 2023/1543**).



In-scope companies

“Service providers” – wide scope e.g.:

- messaging services,
- social networks,
- online marketplaces with user communication features,
- cloud computing services

Key scoping question:

- Does the service provider enable users to communicate with one another **or**
- is data storage and processing by users an essential part of the service?

Important: Companies based outside the EU are also covered, provided the service is aimed at users in the EU market.



Duties to act

In the case of a Production Order

Service provider obligation to produce electronic evidence

- Deadline: **10 days** from receipt of the order
- In urgent cases: **8 hours**

In the case of a Preservation Order

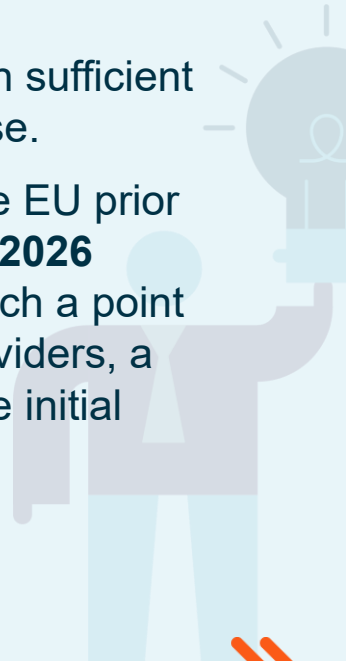
Service provider obligation to preserve electronic evidence **immediately upon receipt** of the order

- Time limit: 60 calendar days from receipt
- Extension by a maximum of 30 days



Point of contact ('addressee')

- In future, service providers must designate a **central point of contact in the EU** responsible for receiving, complying with and enforcing Production and Preservation orders.
- The addressee must be provided with sufficient powers and resources for this purpose.
- For providers already operating in the EU prior to 18 February 2026, the **18 August 2026** deadline to designate and appoint such a point of contact must be met; for other providers, a six-month period applies following the initial provision of services in the EU.



Competent authorities in Germany for European Production Orders

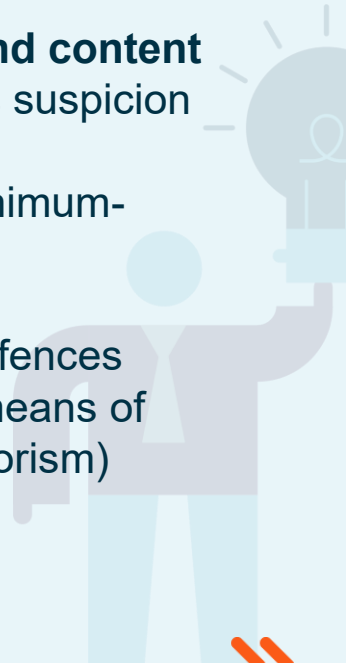
Different rules depending on the data category:

- **Subscriber and identification data:** Where Production Orders issued by the police, amongst others, are permissible, the public prosecutor's office is involved for validation purposes (Sec 9 EBewMG).
- **Traffic and content data:** The European Production Order is generally issued by the court, which sends the certificate directly to the addressee (Sec 10 EBewMG).
- **The enforcement authority** in Germany is the relevant public prosecutor's office (Sec 11 EBewMG).



Conditions for issuing orders

- Orders for the disclosure of **subscriber and identification data**, as well as preservation orders, may be issued where **any criminal offence** is suspected.
- Orders for the disclosure of **traffic and content data** are only possible where there is suspicion of:
 - Criminal offences carrying a minimum-maximum sentence of 3 years' imprisonment
 - Certain categories of criminal offences (e.g. fraud involving non-cash means of payment, terrorist offences, terrorism)



Requirements: What must the service provider do?

- **Review** of the relevant order:
 - Are there any formal errors?
 - Is there any missing information regarding the identity of the person / requested data?
- **Communicate** any factual or legal **impediment to comply with order** to the authority via the notification form.
- **Take into account procedural specifics** depending on the data requested (user, traffic, identification and content data).
- **Implement technical and organisational measures** to ensure confidentiality, secrecy and integrity when complying with order.



Penalties: What are the consequences of breaching obligations?

- Depending on the nature of the breach, fines of up to **EUR 500,000** may be imposed.
- Even failing to name an addressee can constitute an offence.
- For larger service providers (with a total turnover of more than EUR 5 million or EUR 25 million), the fine for certain breaches can amount to up to **2% of total global turnover**.



Need advice or have specific questions?

We support your company in preparing for e-evidence – from the initial risk assessment right through to a legally compliant response to incoming orders. Drawing on our interdisciplinary experience in criminal law and data protection law, we support you with a tailored approach to communicating with law enforcement agencies.



Dr Bettina Enz
Counsel



Sarah Bohn
Associate



Neil Simon-Weaver
Senior Associate