EUROPEAN JUDICIAL NETWORK

Fiches Belges on electronic evidence

Germany

1. **Definition of electronic evidence**

   Electronic evidence means all information, stored or transmitted in a digital form, which is relevant for a specific criminal investigation.

2. **Which measures are possible in your Member State under International Judicial Cooperation?**

   Between the Member States of the European Union all measures are possible which could also be taken in a German proceedings. This includes also the expedited preservation and the expedited disclosure of traffic data.

3. **Procedure for obtaining electronic evidence**
   a. National procedures
   b. international procedures (including Available channels/ways to obtain electronic evidence from your Member State; urgent procedures; specialised networks to obtain electronic evidence e.g. 24/7 Budapest Convention/police channels)

a.
Electronic evidence is obtained in particular through the search and seizure of media, on which or where digital data is stored, and through the collection of digital data (subscriber data, traffic data and content data) via the involvement of the service provider.

b.
The Federal Criminal Police Office is part of the 24/7 network for urgent matters and will contact also in urgent cases provider and/or prosecutor offices in charge. As each prosecution office has a 24/7 service, a prosecutor from the competent prosecutor´s office can always be reached.

The competent public prosecutor´s office is the one in whose area of competence the requested measure is to be carried out. The competent prosecutor´s office can be found via the Atlas of the EJN. The contact points of the EJN will also help to find the correct competent prosecutor´s office.

4. **International legal framework applicable for this measure in your Member State**

- Budapest Convention
- European Investigation Order (EIO) or – where in the EU is not implemented - EU Convention on Mutual Assistance in criminal matters between the member states of the European Union (29 May 2000);

5. **Competent authority to receive and execute your request**

Public Prosecutor´s Office

6. **accepted languages**

German

7. **Definition of data category and examples: subscriber, traffic/transaction and content data in terms of requirements and thresholds for access to data needed in specific criminal investigations**

The subscriber data includes data that the provider stores for the owner of an account in order to be able to properly process the contract, e.g.

Telephone number or mailbox identifier,
Name and address of the holder,
Date of birth,
Date of contract start and end,
Contract information and tariff characteristics.

Insofar as it is necessary to establish the facts or determine the whereabouts of an accused person, information on subscriber data may be requested from any person providing or collaborating in the provision of telecommunications services on a commercial basis.

The information may also be requested by reference to an Internet Protocol address assigned to a specific time.

No threshold exists in relation to the subscriber data and IP-addresses.

Traffic data includes inter alia phone number or other identifier of the calling and called connection or the respective terminal equipment, personal authorization identifiers, the card number for customer cards and the location identifier of the sender or recipient for mobile connections. Furthermore it includes inter alia the start and end of the connection according to the date and time, the amount of data transmitted, the protocol used, the format of the message, the network from which the message originates or to which it is sent, the telecommunication service used, and the endpoints of committed ones connections as well as their time and duration and other connection data required for the establishment and maintenance as well as for payroll accounting.

Threshold:
Orders for the release of traffic data are subject to strict requirements. According to Section 100g of the German Code of Criminal Procedure, they may only be released

- if someone is suspected of a criminal offense "of considerable importance, even in individual cases" (such as e.g. murder, homicide, distribution, acquisition or possession of youth or child pornography, robbery, fraud, computer fraud etc.) or

- if he is suspected to have committed an offence by means of telecommunications.

Moreover, the collection of particularly sensitive traffic data must be necessary for the investigation of the facts of the case and the collection of the data must be proportionate to the importance of the matter.

Content data is any data stored in a digital format related to the content of a communication (text, voice, videos, images and sound other than subscriber or traffic data)

Threshold:
Due to the intervention-intensive character, content data can only be obtained via telecommunication surveillance if
1. certain facts give rise to the suspicion that a person has, either as an offender or participant, committed a specific serious crime of the kind referred to in Section 100a par. 2 of the German Code of Criminal Procedure
2. the offence is one of particular severity in the individual case as well and
3. other means of establishing the facts or determining the accused's whereabouts would be much more difficult or would offer no prospect of success.

8. Voluntary-disclosure:

a. As issuing state: Admissibility of the electronic evidence obtained by voluntary disclosure.

Electronic evidence obtained by voluntary disclosure is admissible.

b. As executing state: Procedures/legislation in your Member State with regards to the possibility for the OSPs in your Member State to provide data directly to other Member States

N/A

9. Data retention periods (including procedures for extensions)

The German law provides for retention periods between 4 and 10 weeks
(4 weeks for location data of the participants of all mobile phone calls at the beginning of the call and location data at the beginning of mobile internet use;
10 weeks for phone numbers, time and duration of all phone calls, sending and receiving times of all SMS messages, assigned IP addresses of all Internet users as well as time and duration of Internet use);
However, the application of the data retention provisions in Germany is currently suspended as the German Bundesverwaltungsgericht has decided to transfer the final interpretation of the data protection guideline for electronic communication (guideline 2002/58 / EG) to the CJEU. Until the final clarification of the CJEU, the data retention provisions in Germany

remain suspended and data is only stored as long as this is necessary for billing purposes. This storage time differs from provider to another.

10. Procedure for data preservation/execution deadline

A court order is necessary for the data preservation. The locally competent prosecutor´s office is competent to request for the court order. The court order is always executed with priority and has in any case to be executed in the time limits set out under question 9.

The storage of the seized data is not subject to a time limit as long as an EIO/MLA-request will be sent.

11. Procedure for data production/ execution deadline

A court order is necessary for the data production. As to the procedure the same applies as set out under question 10.

12. Concise legal practical information

In order to receive traffic and content data it is necessary to describe exactly the offence at stake, the data which shall be retained, the duration of the surveillance, the type of information to be collected and the necessity for the measure in relation to the investigation.