EUROPEAN JUDICIAL NETWORK

Fiches Belges on electronic evidence

Denmark

1. Definition of electronic evidence

In Denmark there is not established any official definition of electronic evidence. However, electronic evidence is considered to refer to various types of data in electronic form (historical or streaming) — including 'content data' such as e-mails, text messages, photographs and videos - often stored on the servers of online service providers, as well as other categories of data, such as subscriber data or traffic information regarding an online account. However, this definition is not necessarily exhaustive.

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

a. Expedited preservation (Art. 29 Budapest Convention)
b. Expedited disclosure of traffic data (Art. 30 Budapest Convention)
c. Production orders/access to data (Art. 31 Budapest Convention)
d. General MLA
e. Reciprocity
f. Spontaneous information (Art. 26 Budapest Convention)
g. Trans-border access (Art. 32 Budapest Convention)
h. Spontaneous information (Art. 7 EU Convention)

3. Procedure for obtaining electronic evidence

a. National procedures

In general, criminal investigations and prosecution procedures are regulated in the Danish Administration of Justice Act.

According to the Danish Administration of Justice Act the obtaining of the most types of electronic evidence requires a court order ordering the person who possesses the information to provide the information.

The requirements for such a court order depends on the type of electronic evidence to be obtained.

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)

All requests for the obtaining of electronic evidence has to be made as a request for Mutual Legal Assistance. The only exceptions are requests for preservation of data.

Some requests may – depending on the type of electronic evidence – be sought fulfilled on a voluntarily basis by the Danish authorities.

- **MLA requests** can be sent directly to the district prosecution service covering the location of the person possessing the said data.

- **24/7-channel/network (Budapest Convention): Danish National Police, Interpol Copenhagen:** urgent preservation requests to preserve subscriber information/traffic data/content (only with MLAT-guarantee: the available data will be preserved for 90 days. Therefore, a Danish court order for the release of the information must be given before 90 days from the date of the preservation).

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

- The Budapest Convention
- EU Convention on Mutual Assistance in criminal matters between the member states of the European Union (29 May 2000)
- European Convention on Mutual Assistance in criminal matters (Strasbourg, 1959 and additional protocols)

5. Competent authority to receive and execute your request

For MLA's: The competent public prosecutor's office.

(Central authority: The office of the Director of Public Prosecutions)

For urgent preservation requests: Danish National Police, Interpol Copenhagen

6. Accepted languages

Requests based on the Budapest Convention: Danish, English

Otherwise: Requests from countries other than Austria, France, Germany, Ireland, Norway, Sweden or the United Kingdom must be translated into either Danish or one of the official languages of the Council of Europe – however preferably in Danish or English.

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

- **Subscriber data**

- The subscriber's account or login name
- The subscriber's name and street address
- The subscriber's telephone number or numbers
- The subscriber's email address
- The Internet Protocol (IP) address used by the subscriber to register the account or otherwise initiate service

- All IP addresses used by the subscriber to log into the account
- Session times, dates and duration
- Any other information pertaining to the identity of the subscriber, including, but not limited to billing information (including type and number of credit cards, student identification number, or other identifying information).

Legal Requirements:

A person (including a Legal Person), who is not a suspect, can be ordered by the court to produce or surrender information/data (disclosure), if:

- The investigation concerns an offence, which is subject to public prosecution by the Danish State (if it was committed in Denmark), and
- There is reason to presume that an object (data), of which the individual has possession, can serve as evidence.

- **Traffic data**

Connection information for other systems to which the user connected via the email account/web host account), including:

- Connection destination or source of connection
- Connection time and date
- Disconnect time and date
- Method of connection to system (e.g. telnet, ftp, http)
- Data transfer volume (e.g. bytes)
- Any other relevant routing information
- Source of destination of any electronic mail messages sent from or received by the account, and the date, time, and length of the message
- Information pertaining to any image(s) or other documents uploaded to the account/website, including the dates and times of upload, and the size of the files
- Name and other identifying details of individuals that accessed a specific image/file/web page in a specified period of time, on a specific date

Legal Requirements:

A person (including a Legal Person), who is not a suspect, can be ordered by the court to produce or surrender information about which communication devices are or has been connected with a certain communication device, even though the owner thereof has not granted permission hereto, if:

- There are specific reasons to presume that messages are given or mail is delivered by the means in question to or from a suspect,
- The invasion is presumed to be of crucial importance to the investigation, and either
- The investigation concerns an offence, which under the Danish law can be punished with imprisonment for six years or more, or concerns one of numerous listed offences

- **Content data**

- For e-mail and web hosting accounts: The content of all emails stored in the account, including copies of emails sent from the account and drafts
- For social media: All communications and messages made or received by the user, including all private messages, attachments (video, audio and picture), group memberships and events

Legal Requirements:

A person (including a Legal Person), who is not a suspect, can be ordered by the court to produce or surrender content data if:

- An individual on reasonable grounds is suspected of an offence, which is subject to public prosecution by the Danish State (if it was committed in Denmark), and
- The production or surrender of the data must be presumed to be of significant importance to the investigation, and
- It is further required, either that the case concerns an offence, which under the Danish law can result in imprisonment, or that there are specific reasons to presume that evidence in the case, which can be surrendered, can be found.

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

      There exists no general issues regarding the admissibility of the electronic evidence obtained by voluntary disclosure, if documentation is provided about how the evidence has been obtained.

   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.

      Direct contact or Direct cooperation between OSPs/ISPs situated in Denmark and a judicial authority of another Member State is not allowed.

9. Data retention periods (including procedures for extensions)

The legal retention period is 1 year. There exists no access for extension.

10. Procedure for data preservation/execution deadline

The period for preservation cannot exceed 90 days, and cannot be extended.

11. Procedure for data production/ execution deadline

Based on the receipt of a MLA, the competent district prosecution service will request the court for an order on the production/surrender of the said data. Based on the court order the possessor of the data will be requested to surrender the data to the police.

12. Concise legal practical information

-