EUROPEAN JUDICIAL NETWORK

Fiches Belges on electronic evidence –

AUSTRIA

1. Definition of electronic evidence

The Austrian Code of Criminal Procedure (CCP) contains no explicit general definition of "electronic evidence". The CCP, however, uses the following definitions:

1. **'disclosure of subscriber data and access data'** (see Section 76a CCP);
2. '**disclosure of data concerning transmission of messages**' as the providing of information about usage data, access data and geo-tracking data of a telecommunication provider or an Information Society service (definition in Section 134 para 2 CCP),
3. '**localizing a technical device**' as the use of technical equipment to ascertain geographic locations and the international mobile subscriber identity (IMSI) numbers without involving a provider or other service providers (definition in Section 134 para 2a CCP),
4. **'event-specific data storage'** as omitting to delete the data listed in subpara. 2 (definition in Section 134 para 2a CCP) (so called **"Quick Freeze"**);
5. '**surveillance of communication**' as monitoring communication and information sent, transmitted or received by a natural person via a communication network or an Information Society service (definition in Section 134 para 3 CCP).

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

Generally, every measure can be executed based on a mutual legal assistance request or EIO provided that the requested measure exists and it could be ordered in a similar domestic case in accordance with the CCP. The EIO-Directive 2014/41/EU sets out several exceptions from the principles mentioned.

The Budapest Convention (CETS No 185) applies directly in Austria. Therefore, all measures provided in Chapter III on International cooperation are applicable. According to the Austrian declaration to Art 29 para 4 of the Budapest Convention dual criminality is required for the execution of the request.

3. Procedure for obtaining electronic evidence

a. National procedures

The procedure for the **disclosure of subscriber data and certain access data** (Section 76a CCP, see below) Is as follows:

Communication services providers are obligated to disclose the **subscriber data** of users (see the categories of data below) at the request of criminal investigation authorities, prosecution authorities, and courts concerning inquiries into concrete suspicions against a particular person for a criminal offence.

The same applies, at the direction of prosecution authority, to the disclosure of the following data *(access data)* of the owner of the technical facility concerned:

1. name, address, and user identification of the user to whom a public IP address was assigned at a particular point in time stating the underlying time zone, unless this assignment would capture a larger number of people;
2. the user identification assigned to the user by email providers;

3. name and address of the user to whom an email address was assigned at a particular time, and
4. the email address and public IP address of an email sender.

"Localizing a technical device" must be ordered by the prosecution authority.

The **other investigative measures (disclosure of data concerning transmission of messages, localizing a technical device** and **surveillance of communication**) must be ordered by the prosecution authority with approval by the court (the substantive requirements are regulated by § 135 CCP, the procedure is specified in §§ 137 – 140 CCP, see question 7).

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)

- In order to find the competent authorities for the execution of Mutual Legal Assistance Requests or EIO consult the EJN-Atlas

- Central authority under Art. 27 para. 2 Cybercrime Convention is:
  Bundesministerium für Justiz (Federal Ministry of Justice)
  Abt. IV 4 Internationale Strafsachen (International Criminal Matters)
  1070 Wien, Museumstrasse 7
  Tel.: +43 1 52 1 52-0
  E-Mail: team.s@bmj.gv.at"

- Austria has designated the following 24/7-point of contact according to Art 35 of the Budapest Convention:
  Bundesministerium für Inneres (Federal Ministry of the Interior)
  Bundeskriminalamt (Federal Criminal Police Office)
  Büro 5.2 Cyber-Crime-Competence-Center
  Josef Holaubek-Platz 1
  1090 Wien

4. International legal framework applicable for this measure in your Member State
   - Convention on Cybercrime (ETS No. 185 "Budapest Convention")
   - European Convention on Mutual Assistance in Criminal Matters (ETS No. 030) and its additional protocols (ETS No. 099 and ETS No. 182)
   - European Investigation Order
   - UN-Treaties applicable in the field of Mutual Legal Assistance
   - In absence of a treaty: MLA on the basis of the principle of reciprocity
5. competent authority to receive and execute your request
   For EIO and Mutual Legal Assistance requests: Public Prosecutor´s Offices locally competent for the execution, i.e. in most cases at the seat of the Internet Service Provider – addresses can be found in the EJN-Atlas.
6. accepted languages
   - For EIO:
     German and any other language based on reciprocity (i.e. if the issuing State accepts EIO from Austria in German language)

- Under the CoE Treaties Framework:
  German, English and French

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

When using the system of categories of data the Austrian CCP follows the definitions in the Austrian Telecommunications Act (Section 92 para 3):

"Subscriber data" (Stammdaten) means all personal data required for the establishment, processing, modification or termination of the legal relations between the user and the provider or for the production and publication of subscriber directories, including

a) name (surname and first name in the case of natural persons, name or designation in the case of legal entities);
b) academic degree in the case of natural persons;
c) address (address of residence in the case of natural persons, place of establishment or billing address in the case of legal entities);
d) subscriber number and other contact information for the message, e) information about manner and content of the contractual relationship,
f) credit-worthiness;

For information on requirements and thresholds for obtaining subscriber and access data un-der § 76a CCP please see answer to question 3a

"Traffic data" (Verkehrsdaten) means any data processed for the purpose of the conveyance of a communication on a communications network or for the billing thereof;

"Access data" (Zugangsdaten) means the traffic data created at the operator during access by a subscriber to a public communications network and required for assignment to the subscriber of the network addresses used for a communication at a specific point of time;

"Content data"(Inhaltsdaten) means the contents of conveyed communications;

"Location data" (Standorddaten) means any data processed in a communications network or by a communications service, indicating the geographic position of the telecommunications terminal equipment of a user of a publicly available communications service; in the case of fixed-link telecommunications terminal equipment, location data refer to the address of the equipment;

With regard to the necessary thresholds **Section 135 para 2** of the Austrian CCP reads as follows:
"D**isclosure of data concerning transmission of messages"** within the above-mentioned definition (i.e. usage data, access data and geo-tracking data) is permissible according to Section 135 para. 2 CCP,

1. if and so long there is strong suspicion that the person affected by the disclosure has kidnapped or otherwise taken control of another person and if the disclosure of data is limited to messages believed to be transmitted, received, or sent by the accused during the deprivation of liberty,

2. if it is to be expected that the disclosure can contribute to inquiries about a criminal offence committed intentionally and punishable by imprisonment for more than six months and if the owner of the technical device that is or will be the source or destination of the transmission of messages expressly consents to the disclosure, or
3. if it is to be expected that the disclosure can contribute to inquiries about a criminal offence committed intentionally and punishable by imprisonment for morethan one year and if because of particular material facts it is believed that through the disclosure data of the accused can be investigated.
4. if because of particular material facts it is expected that through the disclosure the whereabouts of an accused who has absconded or is absent and who is under strong suspicion of having intentionally committed a criminal offence punishable by imprisonment for more than one year can be established.

Localizing a technical device' is only permissible in the cases listed in Sec 135 para 2 subparas. 1, 3 and 4 CCP.

'Event-specific data storage' is permissible based on a reasonable suspicion if this appears necessary to ensure a direction under Sec 135 para. 2 subparas. 2 to 4 CCP.

`Surveillance of communication` is permissible,
1. in cases under Sec 135 para. 2 subpara. 1 CCP,
2. in cases under Sec 135 para. 2 subpara. 2 CCP if the owner of the technical device that is or will be the source or destination of the transmission of messages consents,
3. if this appears necessary for the inquiry about a criminal offence committed intentionally and punishable by imprisonment for more than one year or if the inquiry or prevention of a criminal offence committed or planned as part of a criminal association, terrorist association, or criminal organization would otherwise be significantly obstructed and
    a. if the owner of the technical device that is or will be the source or destination of the transmission of messages is under strong suspicion for a criminal offence committed intentionally and punishable by imprisonment for more than one year or for a criminal offence under §§ 278 to 278b of the Criminal Code, or
    b. because of particular material facts it is believed that the person under strong suspicion for the offence (lit. a) will be using or will establish a connection to the technical device;
4. in cases under Sec 135 para. 2 subpara. 4 CCP.

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

In principle admissible. The Austrian Federal Law on Extradition and Mutual Legal Assistance allows for direct requests to Internet Service Providers abroad for the production of Master data (within the definition above) if

- the data are necessary for the prevention or investigation or prosecution of a criminal offence or for the execution of a sentence and
- the public interest on the request overweighs the fundamental rights of the person concerned and
- the involvement of the competent authority in the requested State would be ineffective or inappropriate.

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
Not available under Austrian law.

9. Data retention periods (including procedures for extensions)

Currently Austria does not have any data retention legislation in force. Following the decision of the ECJ in Digital Rights Ireland, the Austrian regime was repealed by the Austrian Constitutional Court in its decision of June 27th, 2014 (file no. G 47/2012-49, G 59/2020-38, G 62/2020-46, G 70/2020-40, G 71/2010-36). Even if there is no data retention regime in force in Austria, law enforcement authorities can access data that has been stored by the providers for billing purposes. According to -section 99 para 2 of the Federal Act enacting the Telecommunications Act (Telecommunications Act – TKG 2003) the operator of a public communications network or service shall store traffic data to the extent required for the purposes of retail or wholesale billing. The traffic data are to be deleted or made anonymous as soon as the payment process has been completed and the charges have not been contested in writing within a period of three months. For that reason the retention period is, in general, three months. As according to § 99 para 2 TKG 2003 the data are not to be deleted until the end of the period during which a bill may be legally contested in cases where a timely objection is raised (subpara 1), until the end of the period in which payment can be pursued in cases where the bill is not settled (subpara 2) or until a final decision is issued in cases where a procedure is initiated regarding the amount of the charges (subpara 3), the retention period could be longer.

Under EE presidency, Austria presented a different model ("Quick Freeze") which was not a legislative proposal concerning data retention, but rather gives an opportunity to refrain from deletion of data stored for billing purposes for a maximum time period of 12 months (“event-specific data storage”).

10. Procedure for data preservation/execution deadline

As mentioned in 9. above the OSPs do not store data for criminal proceedings. Under the requirements mentioned in 7. above law enforcement authorities can access data that has been stored by the providers for billing purpose. The “event specific data storage” (“Quick Freeze”) does not oblige the OSPs to store the data, but oblige them not to delete the data. The Event-specific data storage is permissible based on a reasonable suspicion (§ 1 para. 3 CCP) if this appears necessary to ensure a direction under para. 2 subparas. 2 to 4 (see under 7.) or a direction under § 76a para. 2. CCP (Note: § 76a CCP refer to subscriber data. According to § 76a CCP communication services providers are obligated to disclose the subscriber data of users (§ 90 para. 7 Telecommunications Act [Telekommunikationsgesetz (TKG)] at the request of criminal investigation authorities, prosecution authorities and courts concerning inquiries into concrete suspicions against a particular person for a criminal offence. The same applies, at the direction of prosecution authority (§ 102), to the disclosure of the following data listed in § 99 para. 5 subpara. 2 of the Telecommunications Act of the owner of the technical facility concerned:
1. name, address, and user identification of the user to whom a public IP address was assigned at a particular point in time stating the underlying time zone, unless this assignment would capture a larger number of people;
2. the user identification assigned to the user by email providers;
3. name and address of the user to whom an email address was assigned at a particular time, and
4. the email address and public IP address of an email sender.).

EUROPEAN
JUDICIAL NETWORK

11. Procedure for data production/ execution deadline

For the legal provisions and procedures see no. 7. above.
“

12. Concise legal practical information

Since Austria is Party to the Convention on Cybercrime (ETS No. 185 “Budapest Convention”) the measures provided for in therein are available under International Judicial Cooperation. According to the Austrian declaration to Art 29 para 4 of the Budapest Convention dual criminality is required for the execution of the request.

Currently Austria does not have any data retention legislation in force. Following the decision of the ECJ in Digital Rights Ireland, the former Austrian regime was repealed by the Austrian Constitutional Court in its decision of June 27th, 2014 (G 47/2012-49, G 59/2020-38, G 62/2020-46, G 70/2020-40, G 71/2010-36). Even if there is no data retention regime in force in Austria, law enforcement authorities can access data that has been stored by the providers for billing purposes. The retention period is, in general, 3 months. § 135 para. 2b CCP gives an opportunity to refrain from deletion of data stored for billing purposes for a maximum time period of 12 months (see above “event-specific data storage”).