EUROPEAN JUDICIAL NETWORK

Fiches Belges on electronic evidence

Sweden

1. Definition of electronic evidence

Sweden has no legal definition of electronic evidence

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

All measures that are possible in a domestic case are possible under international judicial cooperation using a European Investigation Order for countries who have implemented the EIO directive or a request for Mutual Legal Assistance for all other countries. The measures possible are e.g. search and seizure, request for subscriber information and secret interception of telecommunication (both traffic data and content). As of April 1st 2020 it is also possible to request secret data interception, which is used to circumvent encryption for serious offences.

3. Procedure for obtaining electronic evidence

a. National procedures

Search and seizure are decided by the prosecutor in cases regarding crimes where imprisonment could follow. For all use of coercive measures, the principles of purpose, need and proportionality apply. Regarding procedures for other measures, 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)

After an EIO or a request for MLA has been received it will be executed according to the same procedures as in a domestic case. If the requesting country wants the order or the request to be executed according to certain procedures in order to be admissible according to their system, Sweden will try to accommodate the request as long as it isn´t in violation of Swedish law.

There are no specific procedures for urgent requests but they can often be executed very fast. On law enforcement level there is a Swedish Cybercrime Centre at the Police Authority´s National Operations Department which is connected to the 24/7 network.

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

EU Directive 2014/41/EU, with the European Investigation Order (EIO), was implemented in Sweden December 1 2017.

For countries who have not implemented the EU Directive:

- 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);
- Several other bilateral and multilateral treaties.

5. competent authority to receive and execute your request

Requests from EU countries:
National Unit against organised Crime, P.O. Box 57, SE101 21 Stockholm, Sweden

Requests from non-EU countries:
Ministry of Justice, Division for Criminal Cases and International Judicial Cooperation, Central Authority, SE103 33 Stockholm, Sweden

6. accepted languages

The EIO should be written in or translated to Swedish, but English can be accepted if the prosecutor or judge handling the case accepts it.

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

Subscription data is data which is used to identify a subscriber and comprise, for example, subscribers' numbers, names, titles and addresses. Such data are also usually deemed to include information about contracts and billing, for example. Moreover, this category includes information on which fixed or dynamic ip address a subscriber has used or IMSI numbers (those are associated with subscribers' SIM cards and thus telephone numbers), and several other particulars.
Threshold Access to subscription data does not require any court decision; the decision is taken by either the prosecutor in charge of the case or the law enforcement agency itself. Nor is the crime required to be of a particular degree of seriousness.

Traffic data refers in this context, simply expressed, to the data needed to convey an electronic message in an electronic communications network, or to invoice for such a message, e.g. source and destination of the IP address, date, time, duration, route etc. Besides the concept of 'traffic data', the expression location data is also used, to denote data associated with the location of a communication device. It may, for example, be about the cell (base station antenna) to which the equipment is connected.
Threshold Access to traffic and location data in the criminal investigative process requires court decisions and is possible only in cases of serious crime. For all use of coercive measures, the principles of purpose, need and proportionality apply. Consequently, the coercive measures may be used only for the purpose specified in the legislation, if there is an obvious need and a smaller intervention measure is insufficient. In addition, the measure must be in reasonable proportion to both the benefit resulting from, and the intrusion or harm entailed by, the measure. In case of a request for traffic data in an EIO or MLA an explanation from the issuing state regarding purpose, need and proportionality in relation to the investigation is desirable.

Content data is the content of the exchanged messages regardless of format, e.g. text, pictures, videos, voice etc.
Threshold Access to content data in the criminal investigative process also requires court decisions and is possible only in cases of very serious crime with a minimum of 2 years imprisonment. As mentioned regarding traffic data, for all use of coercive measures, the principles of purpose, need and proportionality apply. Consequently, the coercive measures may be used only for the purpose specified in the legislation, if there is an obvious need and a smaller intervention measure is insufficient. In addition, the measure must be in reasonable proportion to both the benefit resulting from, and the intrusion or harm entailed by, the measure. In case of a request for traffic data in an EIO or MLA an explanation from the issuing state regarding purpose, need and proportionality in relation to the investigation is desirable.

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

    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

    It is not possible for the Swedish OSPs to provide data directly to other Member States

9. Data retention periods (including procedures for extensions)

Location data for mobile phone calls: 2 months

Data on internet access: 10 months (except for data identifying the equipment where the communication is finally separated to the subscriber)

All other non-content data: 6 months

10. Procedure for data preservation/execution deadline

N/A, Sweden has no rules on data preservation yet

11. Procedure for data production/ execution deadline

N/A

12. Concise legal practical information

Sweden has not ratified the Budapest Convention yet