EUROPEAN JUDICIAL NETWORK

1. **Definition of electronic evidence.**

There is **no official definition** of electronic evidence in Poland.
All electronic evidence falls under the legal category of **physical evidence**. For this reason, the legal instruments used to collect physical evidence should be applied to electronic evidence, according to Article 236a of the Polish Code of Criminal Procedure. This article states that the provisions used to obtain physical evidence apply accordingly to the holder and user of a device containing **electronic data** or of an **IT system**, with regard to the **data stored** on this device or in this system or on a data storage medium in their possession or use, including correspondence sent by e-mail.

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

In Poland, the following measures are possible:
a. European Investigation Order or MLAR
b. Expedited preservation (Article 29 Budapest Convention)
c. Expedited disclosure of traffic data (Article 30 Budapest Convention)
d. Production orders/access to data (Article 31 Budapest Convention)
e. Spontaneous information (Article 26 Budapest Convention)

3. **Procedure for obtaining electronic evidence:**

a. **National procedures:**

According to the Polish Code of Criminal Procedure, offices, institutions, and entities carrying out telecommunications activities or supplying electronic services and providers of digital services are under an obligation to immediately secure, upon **demand of a court** or a **public prosecutor** contained in a decision, for a specific period of time not longer than **90 days**, IT data stored on devices containing such data on a carrier or in an IT system.
In cases concerning some offences:
- prohibition on propagation of paedophilic behaviour (Article 200b),
- pornography (Article 202 § 3, 4, 4a, 4b) or
- dissemination of content likely to facilitate the commission of a terrorist offence (Article 255a) of the Polish Criminal Code and
- in Chapter 7 **(Criminal provisions)** of the Act of 29 July 2005 on Counteracting Drug Addiction, the obligation to secure data mentioned above may be combined with the **obligation to prevent access** to these data (Article 218a § 1).

The electronic data, which are irrelevant for criminal proceedings, should be released from seizure immediately.

The above provisions shall apply accordingly to securing contents published or made available electronically, with the stipulation that the entity obliged to enforce the demand made by a court or a public prosecutor may also be the controller of these contents.

If the publication or granting of access to contents was a prohibited act, the court or the public prosecutor may order the deletion of the said contents and impose an

obligation to execute the decision on entities: offices, institutions, entities carrying out telecommunications activities or supplying electronic services, providers of digital services or controller of contents.

Polish criminal procedure defines specific **legal measures** for the obtaining of electronic evidence, depending on the type of evidence available.

Depending on the circumstances, one of the two main legal means of obtaining material evidence under the Polish Criminal Procedure Code may be appropriate:

a) By **„seizing objects"** that may serve as evidence (Chapter 25, Article 217)

Objects which may serve as evidence, or be subject to seizure in order to secure financial penalties, criminal measures involving property, forfeiture, compensation measures, or claims to redress damage shall be surrendered when so required by **the court**, **the public prosecutor**, and in cases of utmost urgency, by **the Police** or other authorised body.

A person holding the objects subject to surrender shall be called upon to release them voluntarily.

In the case of refusal to surrender an object voluntarily, its seizure may be enforced.

b) Through the **„search" procedure** (Chapter 25, Article 219)

A search may be conducted to locate and collect items that may be used as evidence in criminal proceedings.

A search may be carried out in private premises and other places if there is a reasonable suspicion that the objects sought are to be found there.

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)

- Police channels: Europol/Interpol/Sienna/Liaison and foreign liaison officers: to obtain (basic) subscriber information;
- There is a 24/7-channel/network (Budapest Convention): urgent preservation requests to seize volatile subscriber information/traffic data/content;
- General MLAR.

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

With regard to (EU Member) States that have implemented the same instruments, the following legal framework is applicable:
- EU Directive 2014/41/EU - European Investigation Order (EIO),
- Budapest Convention.

For countries who have not ratified nor implemented the above mentioned instruments, the following legal framework can be applicable:
- European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959 and additional protocols),
- 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.

The Circuit Prosecutor's Office - the competent public prosecutor's office is the one in whose territorial jurisdiction the requested measure is to be carried out. The competent public prosecutor's office can be found via the EJN Atlas.

6. Accepted languages

(EIO) Polish, in urgent cases English
(CoE Convention) Polish, English, 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

In the Polish legal system, as well as in international cooperation, the definitions contained in the Budapest Convention, EU Directive 2014/41/EU - European Investigation Order (EIO) and national legislation are used. Examples of collected data include emails, audio/video files, logs, metadata, location data, IP addresses, including ports of instant electronic communications.

8. Voluntary-disclosure:

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

Electronic evidence obtained by voluntary disclosure is admissible, if it has been obtained through official procedures.

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

There is no legal framework for voluntary disclosure in Poland. However, the provisions of the Budapest Convention **are in force** in this matter.

9. Data retention periods (including procedures for extensions)

The issue of **data retention** is regulated by **Article 180a** of the **Telecommunications Act**.

The operator of the public telecommunications network and the provider of publicly available telecommunications services shall be obliged, at their own expense, to retain and store data relating to the network termination point, the telecommunications terminal equipment, the end-user: the initiation and termination of the connection, and the determination of the date and time of the connection and its duration, the type of connection, the location of the telecommunications terminal equipment generated in the telecommunications network or processed by it, on the territory of Poland for **a period**

of 12 months from the day of the connection or failed connection. After the expiry of this period, they are obliged to destroy the data.

The above-mentioned operators shall provide data at the **request of the court** and **the prosecutor** in accordance with the principles and in the manner established by separate regulations. These authorities also include **the police**.

There is **no legislation** in Poland on the retention **period of online data**.

10. Procedure for data preservation/execution deadline

According to the Polish Code of Criminal Procedure, offices, institutions and entities conducting telecommunication activity are obliged, upon the **request of the court or the public prosecutor** expressed in the form of a decision, to immediately secure, for a definite period not exceeding **90 (ninety) days**, said electronic data stored on hardware devices in IT systems or on storage media.

The electronic data, which are irrelevant for criminal proceedings, should be released from seizure immediately.

11. Procedure for data production/ execution deadline

The data production procedure is described in the answers to questions 3, 9 and 10.

Execution deadline: the deadlines mentioned in the Budapest Convention or the EU Directive 2014/41/EU (EIO).

12. Concise legal practical information

N/A