

Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of Subscriber Information

1. BACKGROUND

The Council of Europe [Convention on Cybercrime](#) (also known as the Budapest Convention), which was opened for signature in 2001 and entered into force in 2004, was the first international treaty to focus explicitly on cybercrime and electronic evidence. After 20 years, it remains the most significant one in the area. Currently, 69 countries are Parties to the Budapest Convention, including 26 EU Member States¹.



A review of the Budapest Convention is available in the dedicated SIRIUS Quarterly Review [here](#).

In 2003, the Budapest Convention was extended by an [Additional Protocol](#) (First Protocol) covering offences of racist or xenophobic nature.

Following significant developments in the field of information and communication technology which took place since the adoption of the Budapest Convention, on 17 November 2021, after 4 years of negotiations, the Committee of Ministers of the Council of Europe adopted the [Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence](#) (Second Protocol). The Second Protocol was open for signature by the Parties to the Budapest Convention in May 2022 and will enter into force after being ratified by at least five Parties².

The Second Protocol is accompanied by an [Explanatory Report](#) intended to assist Parties in its application. The Budapest Convention itself is similarly accompanied by an [Explanatory Report](#) with the same aim.

The Second Protocol is intended to enhance cooperation among the Parties, as well as between the Parties and service providers and other entities, for obtaining disclosure of electronic evidence for the purpose of criminal investigations or proceedings³.



More information about the Second Protocol is available in the dedicated SIRIUS Quarterly Review [here](#).

An important provision of the Second Protocol aimed at facilitating cooperation between the Parties and private entities is Article 7, which provides a **basis for direct cooperation** between competent authorities and **service providers in the territory of another Party** for the purpose of **obtaining subscriber information**.



Pursuant to Article 7(9), Parties to the Second Protocol may:

1. **Reserve the right not to apply Article 7.** If a Party reserves its right not to apply Article 7, it is not required to take measures under Article 7(2) for service providers in its territory to disclose subscriber information in response to orders issued by other Parties (see section [Enforceability](#)). A Party that makes a reservation to Article 7 is also **not permitted to issue orders** under the article to **service providers in the territory of other Parties**⁴.

2. **Reserve the right not to apply Article 7 to the disclosure of certain types of access numbers**, if this would be inconsistent with the fundamental principles of their domestic legal system. A Party that makes such a reservation is also **not permitted to issue orders for such numbers to service providers in the territory of other Parties**⁵.

A list of all declarations and reservations can be found [here](#).

¹ <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty-num=185>. All EU Member States, except for Ireland.

² Second Protocol, Article 16.

³ Explanatory Report, para. 25.

⁴ Explanatory Report, para. 122.

⁵ Explanatory Report, para. 123.



The SIRIUS project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under contribution agreement No PI/2020/417-500. This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

This document may not necessarily reflect the official position of the Council of Europe or of the Parties to the Budapest Convention on Cybercrime and does not constitute an authoritative interpretation of provisions of this treaty or its protocols.

Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of subscriber information

By no longer requiring a territorial link with the requesting Party, Article 7 of the Second Protocol goes beyond the scope of Article 18 of the Budapest Convention, which establishes a procedure that provides for direct cooperation between **competent authorities in a Party** and a **service provider offering its services in the territory of such Party** for the purpose of obtaining subscriber information.



More information about the toolbox available under Article 18 of the Budapest Convention is available in the dedicated SIRIUS Quarterly Review [here](#).

Article 7 is **without prejudice to the ability of Parties to enforce orders issued under Article 18 of the Budapest Convention or as otherwise permitted by the Budapest Convention, nor does it prejudice cooperation**, including spontaneous cooperation **between Parties and between Parties and service providers**, through other applicable agreements, arrangements, practices or domestic law⁶.

2. SCOPE

- **Types of crimes covered**

The measure provided for under Article 7 of the Second Protocol is applicable to **specific criminal investigations or proceedings** relating to:

- Criminal offences established in accordance with Section 1 of the Budapest Convention and other criminal offences committed by means of a computer system;
- The collection of evidence in electronic form of a criminal offence; and

- Between Parties to the First Protocol, criminal offences established pursuant to the First Protocol⁷.

Therefore, the specific criminal investigations and proceedings covered include not only cybercrime, but **any criminal offence involving evidence in electronic form**. This means that orders under Article 7 of the Second Protocol apply either where a crime is committed by use of a computer system, or where a crime not committed by use of a computer system (for example a murder) involves electronic evidence⁸.

This is also confirmed in [Guidance Note #13](#)⁹, which states that: “The [Cybercrime Convention Committee (T-CY)] agrees that the procedural law provisions and the principles and measures for international co-operation of the [Budapest Convention] are applicable not only to offences related to computer systems and data but also to the collection of electronic evidence of any criminal offence. This broad scope also applies to the measures of the [Second Protocol].”

- **Data covered**

Article 7 of the Second Protocol applies to the **production of subscriber information**. The term “subscriber information” is defined in Article 18(3) of the Budapest Convention and includes any information held by the administration of a service provider relating to a subscriber to its services (other than traffic data or content data) by means of which can be established:

- The type of communication service used, the technical provisions¹⁰ taken thereto and the period of time during which the person subscribed to the service (Article 18(3)(a));

⁶ Second Protocol, Article 5(7); Explanatory Report, para. 95.

⁷ Second Protocol, Article 2(1); Budapest Convention, Article 14(2)(a)-(c).

⁸ Explanatory Report, para. 33. See also Explanatory Report to the Budapest Convention, paras 141, 243.

⁹ Although not binding, Guidance Notes adopted by the T-CY represent the common understanding of the Parties regarding the use of the Budapest Convention and its protocols, see <https://www.coe.int/en/web/cybercrime/guidance-notes>.

¹⁰ The term “technical provisions” includes all measures taken to enable a subscriber to enjoy the communication service, including the reservation of a technical number or address (for example, telephone number, website address / domain name, e-mail address) and the provision and registration of communication equipment used by the subscriber (for example, telephone devices, call centres, LANs). See Explanatory Report to the Budapest Convention, para. 179.

Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of subscriber information

- The subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, which is available on the basis of the service agreement or arrangement¹¹ between the subscriber and the service provider (Article 18(3)(b)); or
- Any other information concerning the site or location where the communication equipment is installed, which is available on the basis of the service agreement or arrangement (Article 18(3)(c)).



It is notable that the **definition of "subscriber information"**, as per Article 18(3) of the Budapest Convention, **may also include information that under the domestic law of some EU Member States is considered as traffic data**. As noted above, Article 7(9)(b) **allows Parties to make a reservation** regarding the application of orders under Article 7 to such information.

The provision only covers **stored and existing data** and does not include any future data or existing data which is in transit.

• Entities covered

Article 7 of the Second Protocol applies to **"service providers"**. The term "service provider" is broadly defined in Article 1(c) of the Budapest Convention and includes:

- Any public or private entity that provides to users of its service **the ability to communicate** by means of a computer system; and
- Any other entity that **processes or stores computer data** on behalf of such

communication service or users of such service.

This definition covers both providers of electronic communication services and of internet society services¹².



It is notable that the **definition of "service provider" set out in the EU Electronic Evidence legislative package¹³** is broader than the one set out in the Budapest Convention and includes both service providers as defined in Article 1(c) of the Budapest Convention, as well as entities providing domain name registration services, as referred to under Article 6 of the Second Protocol.

3. DEFINING THE TOOLBOX

If implemented into the domestic law of the Parties, Article 7 of the Second Protocol provides a basis for a competent authority in a requesting Party to **directly order a service provider in the territory of another Party to the Second Protocol to disclose subscriber information** that is **within its possession or control**.

The term **"service provider in the territory of another Party"** requires that the service provider be **physically present** in the other Party. The mere fact that, for example, a service provider has established a contractual relationship with a company in a Party, but the service provider itself is not physically present in that Party, would not constitute the service provider being "in the territory" of that Party¹⁴.

The term **"possession or control"** refers to **physical possession**, as well as to situations where the data is not in the service provider's physical possession but instead **stored remotely but under the service provider's control**.

¹¹ The reference to a "service agreement or arrangement" includes any kind of relationship on the basis of which a client uses the service provider's services. See Explanatory Report to the Budapest Convention, para. 183.

¹² [Guidance Note #10](#), p. 5, footnote 6.

¹³ The EU Electronic Evidence legislative package defines a "service provider" as any natural or legal person that provides to its users electronic communication services; internet domain name and IP numbering services such as IP address providers, domain name registries, domain name registrars and domain

name related privacy and proxy services; and any other information society service that provides the ability to its users to communicate with each other or makes it possible to store or otherwise process data on behalf of the users to whom the service is provided, where the storage of data is a defining component of the service provided to the user ([Electronic Evidence Regulation](#), Article 3(3); [Electronic Evidence Directive](#), Article 2(1)).

¹⁴ Explanatory Report, para. 99.

Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of subscriber information

4. CONDITIONS AND SAFEGUARDS

A - OVERALL SYSTEM OF SAFEGUARDS

- **Purpose limitation**

In addition to what is noted above (see section [Scope](#), in particular types of crimes covered and data covered), orders under Article 7 may only be issued and submitted in the context of “specific criminal investigations or proceedings”, for information that is “needed for” that investigation or proceeding¹⁵. This means that the measure cannot be used for mass or bulk production of data¹⁶.

- **Additional safeguards**

Article 7, paragraphs 3 and 4, specifying the requirements for orders under Article 7 and the supplemental information which should accompany such an order, respectively (see section [Issuing Party](#)), may assist in applying domestic safeguards¹⁷. Additionally, as noted above, Parties may reserve the right not to apply Article 7 to the disclosure of certain types of access numbers, if this would be inconsistent with the fundamental principles of their domestic legal system¹⁸.

B - ARTICLE 13 OF THE SECOND PROTOCOL: CONDITIONS AND SAFEGUARDS

- **Protection of human rights**

Article 13 of the Second Protocol makes a specific reference to Article 15 of the Budapest Convention and requires Parties to ensure that the powers and procedures established under the Second Protocol – thus including the measure provided for under Article 7 – are subject to an appropriate level of protection for human rights and liberties under their domestic law. These include standards or

minimum safeguards arising pursuant to a Party's obligations under applicable international human rights instruments¹⁹.

- **Principle of proportionality**

Article 15(1) of the Budapest Convention also requires Parties to apply the principle of proportionality. This will be done in accordance with each Party's relevant domestic law principles. In the case of European countries, these principles will be derived from the European Convention on Human Rights (ECHR) and related jurisprudence, meaning that the powers of competent authorities must be **proportional to the nature and circumstances of the offence**²⁰. Other Parties may apply related domestic law principles, such as principles of **relevance** (i.e. the evidence sought must be relevant to the investigation or prosecution), **limitations on overly broad orders**²¹ or **exclude their application in cases concerning minor crimes**²².

- **Other conditions and safeguards**

Pursuant to Article 15(2) of the Budapest Convention, applicable conditions and safeguards include, as appropriate, judicial or other independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof. Other safeguards that must be addressed under domestic law include: the right against self-incrimination, legal privileges, and specificity of individuals or entities subject to the measure²³.

- **Public interest, sound administration of justice and rights of third parties**

In accordance with Article 15(3) of the Budapest Convention, when implementing the provisions of

¹⁵ Second Protocol, Articles 2, 7(1).

¹⁶ Explanatory Report, para. 97.

¹⁷ Explanatory Report, para. 219.

¹⁸ Second Protocol, Article 7(9); Explanatory Report, para. 123.

¹⁹ These instruments include the [1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms](#) (ECHR) and its additional protocols (in respect of European states that are parties to them), other applicable human rights instruments, such as e.g. the [1969 American Convention on Human Rights](#) and the [1981 African Charter on Human Rights and Peoples' Rights](#) (in respect of

states in other regions of the world which are parties to them) and the [1966 International Covenant on Civil and Political Rights](#) (Explanatory Report to the Budapest Convention, para. 145).

²⁰ Explanatory Report, para. 97; Explanatory Report to the Budapest Convention, para. 146.

²¹ Explanatory Report, para. 97; Explanatory Report to the Budapest Convention, para. 145.

²² Explanatory Report to the Budapest Convention, paras 146, 174.

²³ Explanatory Report to the Budapest Convention, para. 147.

Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of subscriber information

Article 7, Parties shall first consider the sound administration of justice and other public interests (for example public safety, public health, the interests of victims, respect for private life). To the extent that it is consistent with these interests, consideration shall also be given to the impact of the measure on the rights, responsibilities and legitimate interests of third parties, which may include, for example, protection from liability for disclosure²⁴.

C - ARTICLE 14 OF THE SECOND PROTOCOL: PROTECTION OF PERSONAL DATA

Article 14 of the Second Protocol provides in its paragraphs 2 to 15 a robust system for data protection. This includes safeguards regarding purpose and use of the data; data quality and integrity; sensitive data; retention of data; automated decision-making; security; records and logging; transparency and notice regarding processing, retention periods, data disclosure, access rectification and redress available; right to access and rectification; judicial and non-judicial remedies; and independent oversight²⁵. A Party may also suspend the transfer of personal data to another Party based on substantial evidence of systematic or material breach of Article 14²⁶.

Pursuant to Article 14(1)(a), each Party shall process personal data that it receives under the Second Protocol in accordance with the specific safeguards set out in Article 14(2)-(15), with two exceptions:

1. If, at the time of transfer of data, both the transferring Party and the receiving Party are bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data, which is applicable to the transfer of personal data for the purpose of the prevention, detection, investigation and prosecution of criminal offences (Article 14(1)(b)). This would include, for

example, [Convention 108+](#) and the [EU-US Umbrella Agreement](#)²⁷.

2. If the transferring Party and the receiving Party, not bound by an international agreement as described above, nevertheless agree that the transfer of data under the Second Protocol may take place on the basis of other agreements or arrangements between them in lieu of Article 14(2)-(15). For EU Member States, in relation to transfers of personal data to third countries, such an alternative agreement would have to comply with the requirements of EU data protection legislation.

5. ISSUING PARTY

A- ISSUING AUTHORITIES

Requests under Article 7 of the Second Protocol must be issued by competent authorities²⁸.

The Second Protocol defines the term “competent authority” as a judicial, administrative or other law-enforcement authority that is **empowered by domestic law to order, authorise or undertake the execution of measures under the Second Protocol for the purpose of collection or production of evidence** with respect to specific criminal investigations or proceedings²⁹.

The domestic legal system of a Party will govern which authority is considered as a competent authority to issue an order under Article 7 of the Second Protocol.



Pursuant to Article 7(2)(b), Parties can make a **declaration that orders under Article 7** issued towards service providers located within their territory must be **issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision**. A Party making use of the declaration must accept orders issued by or under the supervision of any of the enumerated authorities.

²⁴ Explanatory Report to the Budapest Convention, para. 148.

²⁵ For more information, see Second Protocol, Article 14(2)-(14) and Explanatory Report, paras 227-281.

²⁶ Second Protocol, Article 14(15).

²⁷ Explanatory Report, para. 222.

²⁸ Second Protocol, Article 7(1).

²⁹ Second Protocol, Article 3(2)(b).

Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of subscriber information

B- ISSUING PROCEDURE

Orders under Article 7 of the Second Protocol are issued by the competent authority directly to the service provider concerned, on the basis of the relevant provisions of the domestic law of the issuing Party.

- **Requirements for orders under Article 7**

Pursuant to Article 7(3), the order must specify:

- The **issuing authority** and the **date** of issuance (Article 7(3)(a));
- A statement that the order is **issued pursuant to the Second Protocol**, i.e. that the order is in accordance with the terms of the Second Protocol³⁰ (Article 7(3)(b));
- The **name and address of the service provider(s)** to be served (Article 7(3)(c));
- The **offence(s)** that is / are the subject of the criminal investigation or proceeding (Article 7(3)(d));
- The **authority seeking the specific subscriber information**, if not the issuing authority³¹ (Article 7(3)(e)); and
- A detailed **description of the specific subscriber information** sought (Article 7(3)(f)).

Article 7(3) **does not include a requirement to include a statement of facts in the order**, considering that this information is confidential in most criminal investigations and may not be disclosed to a private party³².

Parties may always **choose to include additional information** in the order itself to assist in its processing or because this is required pursuant to domestic law³³. Furthermore, while Article 7(3) sets out the **minimum information** required for orders under Article 7, these orders **often can only be executed** if the service provider (and, as applicable, the receiving Party's designated authority pursuant to Article 7(5) of the Second Protocol, see section

[Requested / Transferring Party](#)) is provided with **supplemental information**³⁴. Article 7(4) thus provides that an issuing authority shall provide supplemental information about:

- The domestic legal grounds that **empower the authority to issue the order** (Article 7(4)(a));
- A reference to **legal provisions and applicable penalties for the offence** being investigated or prosecuted (Article 7(4)(b));
- The **contact information of the authority** to which the service provider shall return the subscriber information, from which it can request further information, or to which it shall otherwise respond³⁵ (Article 7(4)(c));
- The **time frame** within which and the **manner in which to return the subscriber information** (Article 7(4)(d));
- Whether **preservation of the data has already been sought**, including the **date of preservation** and any applicable **reference number** (Article 7(4)(e));
- Any **special procedural instructions** (Article 7(4)(f));
- **If applicable**, a statement that **simultaneous notification** (see section [Requested / Transferring Party](#)) to the Party in the territory of which the service provider is located, **has been made** (Article 7(4)(g)); and
- Any **other information that may assist** in obtaining disclosure of the subscriber information (Article 7(4)(h)).

"Special procedural instructions" is intended to include any **request for confidentiality** (including a request for non-disclosure of the order to the subscriber or other third parties) or **authentication**³⁶. However, special procedural instructions **may not**

³⁰ Explanatory Report, para. 102.

³¹ In some Parties, the issuing authority and the authority seeking the data are not the same. For example, investigators or prosecutors may be the authorities seeking the data, while the actual order is issued by a judge. See Explanatory Report, para. 103.

³² Explanatory Report, para. 104.

³³ Explanatory Report, para. 102.

³⁴ Explanatory Report, para. 105.

³⁵ Such contact information does not need to identify a specific individual, but only the office, see Explanatory Report, para. 105.

³⁶ Ibid.

Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of subscriber information

prevent the service provider from consulting with authorities to be notified under Article 7(5)(a) or consulted under Article 7(5)(b) (see section [Requested / Transferring Party](#)). If confidentiality is required to avoid a premature disclosure of the matter, this should be indicated in the order³⁷.



In some Parties, confidentiality of the order will be maintained by operation of the law, while in other Parties this is not necessarily the case. Therefore, in order to avoid the risk of premature disclosure of the investigation, Parties are **encouraged to be aware of applicable law and a service provider's policies concerning subscriber notification**, prior to submitting an order under Article 7.

"Special procedural instructions" may also include specification of the **transmission channel best suited to the requesting authority's needs**³⁸.

The supplemental information under Article 7(4) can be provided separately but may also be included in the order itself if this is permissible under the issuing Party's law³⁹. The service provider may also request additional information regarding the account or other information to assist it in providing a prompt and complete response⁴⁰.

Lastly, pursuant to Article 4(2) of the Second Protocol, orders under Article 7 and any accompanying information shall be:

- Submitted in a language of the other Party in which the service provider accepts such orders under **comparable domestic process**;
- Submitted in another language **acceptable to the service provider**; or
- **Accompanied by a translation** into one of the two above-mentioned languages.

- **Transmission of orders under Article 7**

Article 7(6) **encourages the use of electronic means when acceptable to the service provider**. Accordingly, if acceptable to the service provider, a

Party may submit an order under Article 7 in electronic form, for example by using e-mail, electronic portals or other means. While it is assumed that entities prefer to receive requests in electronic format, **it is not a requirement that this format only may be used**.

Furthermore, appropriate levels of security and authentication may be required. Authentication methods may include a variety of means or a combination thereof, for example, obtaining confirmation of authenticity via a known authority in the issuing Party (such as the sender or a central or designated authority), subsequent communications between the issuing authority and the requested / transferring Party, use of an official e-mail address or future technological verification methods that can be easily used by transmitting authorities⁴¹. The Parties and service providers may decide themselves whether secure channels or means for transmission and authentication are available or whether special security protections (including encryption) may be necessary in a particular sensitive case.

5. REQUESTED / TRANSFERRING PARTY

The Second Protocol uses the term "transferring Party" to refer to, among others, a Party in whose territory a transmitting service provider is located⁴².

The role of the transferring Party will depend on each Party's domestic legislation. However, the Second Protocol sets out a few specificities concerning transferring Parties under Article 7, as further set out below.

- **Notification and consultation requirements**

Article 7(5)(a) of the Second Protocol **allows Parties to make a declaration** that, when an order under Article 7 is made to a service provider within their territory, **simultaneous notification** of the order,

³⁷ A request for confidentiality should also not prevent service providers from transparency reporting on anonymised aggregate numbers of orders received under Article 7, see Explanatory Report, para. 106.

³⁸ Ibid.

³⁹ Explanatory Report, para. 105.

⁴⁰ Explanatory Report, para. 106.

⁴¹ Explanatory Report para. 116.

⁴² Second Protocol, Article 3(2)(e).

Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of subscriber information

the supplemental information and a summary of the facts related to the investigations or proceedings is required, **in every case** (i.e. for all orders transmitted to service providers in its territory) **or in identified circumstances**. Such notification may be provided in electronic form. Appropriate levels of security and authentication may be required⁴³.

Under Article 7(5)(b) of the Second Protocol, a Party may also, **under its domestic law, require a service provider** within its territory that receives an order from another Party **to consult with it in identified circumstances**. A Party may not require consultation for all orders, which would add an additional step that could cause significant delay, but only in more limited, identified circumstances. Consultation requirements should be limited to circumstances in which there is a heightened potential for the need to impose a condition or invoke a ground for refusal, or a concern of potential prejudice to the transferring Party's criminal investigations or proceedings⁴⁴.

The notification and consultation procedures are **entirely discretionary**. A Party is not obliged to require either one⁴⁵. Furthermore, a Party may change its notification or its consultation requirement at any time.

A Party that requires notification or consultation may decide to impose on the service provider a **waiting period** before the provider furnishes the subscriber information in response to the order, in order to permit notification or consultation and any follow-up request by the Party for additional information⁴⁶.

- **Instruction not to disclose**

The authority notified under Article 7(5)(a) or consulted under Article 7(5)(b) may, **without undue delay, instruct the service provider not to disclose** the requested subscriber information if:

- Disclosure may **prejudice criminal investigations or proceedings** in the Party

in which the service provider is located (Article 7(5)(c)(i)); or

- **Conditions or grounds for refusal** would apply under Article 25(4) or Article 27(4) of the Budapest Convention, had the subscriber information been sought through mutual legal assistance (Article 7(5)(c)(ii)).



Article 25(4) of the Budapest Convention refers to **grounds for refusal set out in any applicable mutual assistance** treaties and in domestic law.

Article 27(4) of the Budapest Convention allows for refusal where:

- The request concerns an offence which the requested Party considers a **political offence** or an offence **connected with a political offence**; or
- The execution of the request is likely to prejudice its **sovereignty, ordre public** or other **essential interests**.

Cooperation is in principle to be extensive and impediments thereto strictly limited. Accordingly, the determination by the Party as to which conditions and grounds for refusal would apply **should be limited** in line with the objectives of Article 7 of the Second Protocol to eliminate barriers and provide for more efficient and expedited procedures for cross-border access to electronic evidence for criminal investigations⁴⁷.

- **Request for additional information**

The authority notified under Article 7(5)(a) or consulted under Article 7(5)(b):

- May **request additional information** from the authority to which the service provider shall return the subscriber information, from which it can request further information, or to which it shall otherwise respond (the Requesting Authority) for the purpose of assessing whether any reasons to instruct the service provider not to

⁴³ Second Protocol, Article 7(6).

⁴⁴ Explanatory Report, para. 108.

⁴⁵ Explanatory Report, para. 109.

⁴⁶ Explanatory Report, para. 112.

⁴⁷ Explanatory Report, para. 110.

Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of subscriber information

disclose the requested subscriber information apply and **shall not disclose such additional information to the service provider without the Requesting Authority's consent** (Article 7(5)(d)(i)); and

- Shall **promptly inform** the Requesting Authority **if the service provider has been instructed not to disclose** the subscriber information and **give the reasons** for doing so (Article 7(5)(d)(ii)).

This procedure may provide an opportunity to clarify, for example, aspects of the confidentiality of the information sought, as well as any intended use limitation by the authority seeking the data⁴⁸.

A Party shall designate a **single authority** to receive notification under Article 7(5)(a), be consulted by service providers prior to disclosure under Article 7(5)(b), instruct service providers not to disclose information and request additional information from the Requesting Authority⁴⁹.

An updated **register of the authorities so designated** by the Parties and **whether and under what circumstances they require notification** pursuant to Article 7(5)(a) shall be set up and kept by the Secretary General of the Council of Europe⁵⁰.

6. ENFORCEABILITY

Article 7(2)(a) of the Second Protocol requires each Party to **adopt measures that may be necessary** for service providers in its territory to disclose subscriber information in response to an order under Article 7. Given the differences in domestic legal systems, Parties may implement different measures to establish a procedure for the direct cooperation to take place in an effective and efficient manner. This may range from **removing legal obstacles** for service providers to respond to an order to **providing an affirmative basis, obliging service providers to respond to an order from an**

authority of another Party in an effective and efficient manner⁵¹.

Each Party must ensure that **service providers can lawfully comply with orders under Article 7** in a manner that provides legal certainty. For example, service providers should not incur legal liability for having complied in good faith with an order issued under Article 7, which the requesting Party has stated is issued pursuant to the Second Protocol. This does not preclude liability for reasons other than complying with the order, for example, failure to follow any domestic law requirements.

The form of implementation depends on Parties' respective legal and policy considerations. For Parties that have data protection requirements, such as EU Member States, this would include providing a clear basis for the processing of personal data⁵².

Regardless of the domestic legal measures adopted by the transferring Party, the issuing **Party may only seek enforcement** of an order under Article 7 **pursuant to Article 8 or another form of mutual assistance**⁵³. Parties **may not seek unilateral enforcement** of production orders issued pursuant to the article⁵⁴. They may, however, request that a service provider **give a reason for refusing to disclose** the subscriber information sought by the order⁵⁵. Service providers are encouraged to explain the reasons for not providing the data sought, in order for Parties to be able to assess whether to seek enforcement of the order⁵⁶. For example, should the service provider indicate that the data is no longer available, the issuing Party would no longer pursue other means for obtaining the data.

For enforcement of the order via Article 8, the Second Protocol contemplates a simplified procedure of conversion of an order under Article 7 to an order under Article 8⁵⁷.

An issuing Party may seek enforcement under Article 8 or another form of mutual assistance:

⁴⁸ Explanatory Report, para. 111.

⁴⁹ Second Protocol, Article 7(5)(e).

⁵⁰ Second Protocol, Article 7(5)(f).

⁵¹ Explanatory Report, para. 100.

⁵² Ibid.

⁵³ Second Protocol, Article 7(7).

⁵⁴ Explanatory Report, para. 117.

⁵⁵ Second Protocol, Article 7(7).

⁵⁶ Explanatory Report, para. 119.

⁵⁷ Explanatory Report, para. 118.

Article 7 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Disclosure of subscriber information

- After the **expiry of 30 days**, or of the **time frame stipulated in the order** for its execution, **whichever is longer**;
- If the **service provider has indicated a refusal to comply**, prior to the expiration of the aforementioned time period; or
- If the **authority notified** under Article 7(5)(a) or **consulted** under Article 7(5)(b) has informed the issuing Party that the service provider has been **instructed not to disclose the information** sought, prior to the expiration of the aforementioned time period.



If an authority notified under Article 7(5)(a) or consulted under Article 7(5)(b) has informed the issuing Party that the service provider has been instructed not to disclose the information sought, there is a risk that any further request under Article 8 may likewise be denied. In such an instance, the issuing Party is **advised to consult in advance** with the authorities designated under Article 7(5)(a) or (b) in order to **address any deficiencies** in the original order and to avoid submitting orders under Article 8 or via any other mutual assistance mechanism that may be rejected⁵⁸.

⁵⁸ Explanatory Report, para. 120.