Article 6 of the Second Additional Protocol to the Budapest Convention on Cybercrime: Direct Requests for Domain Name Registration 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 States [1].

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 Parties [2].

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 specific criminal investigations or proceedings [3].

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 6, which provides a basis for direct cooperation between competent authorities and **entities providing domain name registration services in the territory of another Party** for the purpose of **obtaining domain name registration information**. Obtaining such information is often indispensable as a first step for many criminal investigations and to determine where to direct requests for international cooperation [4].

2. SCOPE

- **Types of crimes covered**

The measure provided for under Article 6 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

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

[2] Second Protocol, Article 16.
[3] Explanatory Report, para. 25.
[4] Explanatory Report, para. 73.

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.

- Between Parties to the First Protocol, criminal offences established pursuant to the First Protocol[5].

Therefore, the specific criminal investigations and proceedings covered include not only cybercrime, but **any criminal offence involving evidence in electronic form**. This means that requests under Article 6 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 evidence[6].

This is also confirmed in Guidance Note #13[7], 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 6 of the Second Protocol applies to **domain name registration information**, i.e. information aimed **at identifying or contacting the registrant of a specific domain name**. This refers to information previously publicly available through so-called WHOIS lookup tools, such as the name, physical address, e-mail address and telephone number of a registrant. Some Parties may consider this information a subset of subscriber information as defined in Article 18(3) of the Budapest Convention[8].

In some cases, domain name registration information may be personal data and may be protected under data protection regulations in the Party where the respective entity providing domain name registration services or the person to whom the data relates is located[9]. However, generally, domain name registration information is basic information that would not permit precise conclusions to be drawn concerning the private lives and daily habits of individuals. Its disclosure may, therefore, be less intrusive than the disclosure of other categories of data[10].

- **Entities covered**

Article 6 of the Second Protocol applies to **entities providing domain name registration services**. These include:

- Organisations that sell domain names to the public ("registrars"); and
- Regional or national registry operators, which keep authoritative databases ("registries") of all domain names, registered for a top-level domain and which accept registration requests[11].

> ⚠ It is notable that entities providing domain name registration services, as referred to under Article 6 of the Second Protocol, fall under the **definition of "service provider" set out in the EU Electronic Evidence legislative package**[12].

3. DEFINING THE TOOLBOX

If implemented into the domestic law of the Parties, Article 6 of the Second Protocol provides a basis for direct cooperation between a **competent authority in a requesting Party** and **entities providing**

[5] Second Protocol, Article 2(1); Budapest Convention, Article 14(2)(a)-(c).
[6] Explanatory Report, para. 33. See also Explanatory Report to the Budapest Convention, paras 141, 243.
[7] 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.
[8] Explanatory Report, para. 81.
[9] Explanatory Report, para. 75.
[10] Explanatory Report, para. 81.
[11] Explanatory Report, para. 75.
[12] 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)).

domain name registration services in another Party to the Second Protocol for **disclosure of domain name registration information** which is in that **entity's possession or control**.

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

It is notable that requests for the disclosure of domain name registration under Article 6 of the Second Protocol are **non-binding**, as further explained in section Enforceability.

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), requests under Article 6 may only be issued and submitted in the context of "specific criminal investigations or proceedings", for identifying or contacting the registrant of a domain name[13].

- **Additional safeguards**

Article 6(3), specifying the requirements for requests under Article 6 (see section Issuing Party), may assist in applying domestic safeguards[14].

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 6 – 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 instruments[15].

- **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**[16]. 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). Parties should also avoid broad requests for disclosure of domain name information unless they are needed for the specific criminal investigation or proceeding[17].

- **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 measure[18].

[13] Second Protocol, Articles 2, 6(1).
[14] Explanatory Report, para. 219.
[15] 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 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).
[16] Explanatory Report, para. 84(c); Explanatory Report to the Budapest Convention, para. 146.
[17] Explanatory Report, para. 84(c).
[18] Explanatory Report to the Budapest Convention, para. 147.

- **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 Article 6, 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 disclosure[19].

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 oversight[20]. A Party may also suspend the transfer of personal data to another Party based on substantial evidence of systematic or material breach of Article 14[21].

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[22].
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 6 of the Second Protocol must be issued by competent authorities[23].

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 proceedings[24].

The domestic legal system of a Party will govern which authority is considered as a competent authority to issue a request under Article 6 of the Second Protocol.

B - ISSUING PROCEDURE

Requests under Article 6 of the Second Protocol are issued by the competent authority directly to the entity providing domain name registration

[19] Explanatory Report to the Budapest Convention, para. 148.
[20] For more information, see Second Protocol, Article 14(2)-(14) and Explanatory Report, paras 227-281.
[21] Second Protocol, Article 14(15).
[22] Explanatory Report, para. 222.
[23] Second Protocol, Article 6(1).
[24] Second Protocol, Article 3(2)(b).

concerned, on the basis of the relevant provisions of the domestic law of the issuing Party.

- **Requirements for requests under Article 6**

Pursuant to Article 6(3), the request must include, as a minimum:

- The **date** of the request and the **identity and contact details of the competent authority** issuing the request (Article 6(3)(a));
- The **domain name** about which information is sought and a **detailed list of the information sought**, including the particular data elements (Article 6(3)(b)); these may include the name, physical address, e-mail address or telephone number of a registrant[25];
- A statement that the request is **issued pursuant to the Second Protocol** (i.e. in accordance with the terms of the Second Protocol[26]), that the need for the information arises because of its **relevance to a specific criminal investigation or proceeding** and that the **information will only be used for that specific criminal investigation or proceeding** (Article 6(3)(c)); and
- The time and the manner in which to disclose the information and any other **special procedural instructions** (Article 6(3)(d)).

"Special procedural instructions" is intended to include any **request for confidentiality**, including a **request for non-disclosure of the request to the registrant or other third parties**. If confidentiality is required to avoid a premature disclosure of the matter, this should be indicated in the request[27].

⚠ In some Parties, confidentiality of the request will be maintained by operation of law, while in other Parties this is not necessarily the case. Therefore, where confidentiality is needed, Parties are encouraged to **review publicly available information** and to **seek guidance from other Parties regarding applicable law**, as well as **the policies of the entities providing domain name registration services** concerning subscriber / registrant information, prior to submitting a request under Article 6 of the Second Protocol to the entity[28].

"Special procedural instructions" may also include specification of the **transmission channel best suited to the requesting authority's needs**[29].

Article 6(3) **does not include a requirement to include a statement of facts in the request**, considering that this information is confidential in most criminal investigations and may not be disclosed to a private party. However, **the entity receiving a request** under this article **may need certain additional information** that would allow it to come to a positive decision regarding the request. Therefore, the entity may seek other information **where it cannot otherwise execute the request**[30].

Lastly, pursuant to Article 4(2) of the Second Protocol, requests under Article 6 and any accompanying information shall be:

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

- **Transmission of requests under Article 6**

Article 6(4) **encourages the use of electronic means when acceptable to the entity** providing domain name registration services. Accordingly, if acceptable to the entity, a Party may submit a request under Article 6 in electronic form, for example by using e-mail, electronic portals or other means[31]. An organisation may also provide an interface or lookup tool to facilitate or expedite the disclosure of domain name registration information

[25] Explanatory Report, para. 84(b).
[26] Explanatory Report, para. 84(c).
[27] Explanatory Report, para. 84(d).
[28] Ibid.
[29] Ibid.
[30] Explanatory Report, para. 85.
[31] Explanatory Report, para. 86.

following a request[32]. 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. The Parties and entities 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[33].

6. ENFORCEABILITY

Article 6(2) of the Second Protocol requires each Party to **adopt measures to permit** entities in its territory providing domain name registration services to disclose such information in response to a request under Article 6, subject to reasonable conditions provided by domestic law, which in some Parties may include data protection conditions[34]. However, it **does not require** Parties **to enact legislation obliging** such entities to respond to a request from an authority of another Party[35]. It is therefore up to the entities offering domain name registration services themselves to determine whether to disclose the information sought, within the remits of the applicable laws of the jurisdiction that they submit themselves to. Furthermore, Article 6 gives Parties flexibility regarding the format in which requests are made and a Party can use procedures available under its domestic law, including the issuance of an order. Yet, for the purposes of Article 6, such an order is treated as a **non-binding request**.[36]

Nevertheless, while requests issued pursuant to Article 6 are non-binding, it is **expected that a requested entity will be able to disclose** the information sought pursuant to the provision **where the applicable conditions have been met**.

Furthermore, pursuant to Article 6(5) of the Second Protocol, in the event of non-cooperation, the requesting Party may request that the entity **provide reasons for not disclosing** the information sought. Entities are encouraged to explain the reasons for not disclosing data. The article further providers for **consultation between the Parties** involved with a view to determining available measures to obtain the information, as well as, for example, to improve future cooperation[37].

At the time of signature of the Second Protocol or when depositing its instrument of ratification, acceptance or approval, or at any other time, Parties shall designate an **authority for the purpose of consultation** under Article 6(5)[38]. Providing such a contact point in the Party where the entity is located will assist the requesting Party in quickly determining what measures are available to obtain the data sought, if the entity declines to execute a request made under Article 6[39].

An updated register of the authorities designated by the Parties under Article 6(6) shall be kept by the Secretary General of the Council of Europe[40].

[32] Explanatory Report, para. 78.
[33] Explanatory Report, para. 86.
[34] Explanatory Report, para. 82.
[35] Explanatory Report, para. 83.
[36] Explanatory Report, para. 77.
[37] Explanatory Report, para. 87.
[38] Second Protocol, Article 6(6).
[39] Explanatory Report, para. 88.
[40] Second Protocol, Article 6(7).