

**ZAKON O POTVRĐIVANJU DRUGOG DODATNOG PROTOKOLA UZ KONVENCIJU O
RAČUNARSKOM KRIMINALU O UNAPRIJEĐENOJ SARADNJI I OTKRIVANJU
ELEKTRONSKIH DOKAZA**

Član 1

Potvrđuje se Drugi dodatni protokol uz Konvenciju o računarskom kriminalu o unaprijeđenoj saradnji i otkrivanju elektronskih dokaza, usvojen 12. maja 2022. godine u Strazburu, u originalu na engleskom i francuskom jeziku.

Član 2

Tekst Protokola iz člana 1 ovog zakona, u originalu na engleskom jeziku i u prevodu na crnogorski jezik, glasi:

**SECOND ADDITIONAL PROTOCOL TO THE CONVENTION ON CYBERCRIME
ON ENHANCED CO-OPERATION AND DISCLOSURE OF ELECTRONIC
EVIDENCE**

Preamble

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime (ETS No. 185, hereinafter “the Convention”), opened for signature in Budapest on 23 November 2001, signatories hereto,

Bearing in mind the reach and impact of the Convention in all regions of the world;

Recalling that the Convention is already supplemented by the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), opened for signature in Strasbourg on 28 January 2003 (hereinafter “the First Protocol”), as between Parties to that Protocol;

Taking into account existing Council of Europe treaties on co-operation in criminal matters as well as other agreements and arrangements on co-operation in criminal matters between Parties to the Convention;

Having regard also for the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) as amended by its amending Protocol (CETS No. 223), opened for signature in Strasbourg on 10 October 2018, and to which any State may be invited to accede;

Recognising the growing use of information and communication technology, including internet services, and increasing cybercrime, which is a threat to democracy and the rule of law and which many States also consider a threat to human rights;

Also recognising the growing number of victims of cybercrime and the importance of obtaining justice for those victims;

Recalling that governments have the responsibility to protect society and individuals against crime not only offline but also online, including through effective criminal investigations and prosecutions;

Aware that evidence of any criminal offence is increasingly stored in electronic form on computer systems in foreign, multiple or unknown jurisdictions, and convinced that additional measures are needed to lawfully obtain such evidence in order to enable an effective criminal justice response and to uphold the rule of law;

Recognising the need for increased and more efficient co-operation between States and the private sector, and that in this context greater clarity or legal certainty is needed for service providers and other entities regarding the circumstances in which they may respond to direct requests from criminal justice authorities in other Parties for the disclosure of electronic data;

Aiming, therefore, to further enhance co-operation on cybercrime and the collection of evidence in electronic form of any criminal offence for the purpose of specific criminal investigations or proceedings through additional tools pertaining to more efficient mutual assistance and other forms of co-operation between competent authorities; co-operation in emergencies; and direct cooperation between competent authorities and service providers and other entities in possession or control of pertinent information;

Convinced that effective cross-border co-operation for criminal justice purposes, including between public and private sectors, benefits from effective conditions and safeguards for the protection of human rights and fundamental freedoms;

Recognising that the collection of electronic evidence for criminal investigations often concerns personal data, and recognising the requirement in many Parties to protect privacy and personal data in order to meet their constitutional and international obligations; and

Mindful of the need to ensure that effective criminal justice measures on cybercrime and the collection of evidence in electronic form are subject to conditions and safeguards, which shall provide for the adequate protection of human rights and fundamental freedoms, including rights arising pursuant to obligations that States have undertaken under applicable international human rights instruments, such as the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5) of the Council of Europe, the 1966 United Nations International Covenant on Civil and Political Rights, the 1981 African Charter on Human and People's Rights, the 1969 American Convention on Human Rights and other international human rights treaties;

Have agreed as follows:

Chapter I - Common provisions

Article 1 – Purpose

The purpose of this Protocol is to supplement:

- a the Convention as between the Parties to this Protocol; and
- b the First Protocol as between the Parties to this Protocol that are also Parties to the First Protocol.

Article 2 – Scope of application

1 Except as otherwise specified herein, the measures described in this Protocol shall be applied:

a as between Parties to the Convention that are Parties to this Protocol, to specific criminal investigations or proceedings concerning criminal offences related to computer systems and data, and to the collection of evidence in electronic form of a criminal offence; and

b as between Parties to the First Protocol that are Parties to this Protocol, to specific criminal investigations or proceedings concerning criminal offences established pursuant to the First Protocol.

2 Each Party shall adopt such legislative and other measures as may be necessary to carry out the obligations set forth in this Protocol.

Article 3 – Definitions

1 The definitions provided in Articles 1 and 18, paragraph 3, of the Convention apply to this Protocol.

2 For the purposes of this Protocol, the following additional definitions apply:

a “central authority” means the authority or authorities designated under a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned, or, in the absence thereof, the authority or authorities designated by a Party under Article 27, paragraph 2.a, of the Convention;

b “competent authority” means a judicial, administrative or other law-enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings;

c “emergency” means a situation in which there is a significant and imminent risk to the life or safety of any natural person;

d “personal data” means information relating to an identified or identifiable natural person;

e “transferring Party” means the Party transmitting the data in response to a request or as part of a joint investigation team or, for the purposes of Chapter II, section 2, a Party in whose territory a transmitting service provider or entity providing domain name registration services is located.

Article 4 – Language

1 Requests, orders and accompanying information submitted to a Party shall be in a language acceptable to the requested Party or the Party notified under Article 7, paragraph 5, or be accompanied by a translation into such a language.

2 Orders under Article 7 and requests under Article 6, and any accompanying information shall be:

- a submitted in a language of the other Party in which the service provider or entity accepts them under comparable domestic process;
- b submitted in another language acceptable to the service provider or entity; or
- c accompanied by a translation into one of the languages under paragraphs 2.a or 2.b.

Chapter II – Measures for enhanced co-operation

Section 1 – General principles applicable to Chapter II

Article 5 – General principles applicable to Chapter II

1 The Parties shall co-operate in accordance with the provisions of this Chapter to the widest extent possible.

2 Section 2 of this chapter consists of Articles 6 and 7. It provides for procedures enhancing direct co-operation with providers and entities in the territory of another Party. Section 2 applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned.

3 Section 3 of this chapter consists of Articles 8 and 9. It provides for procedures to enhance international co-operation between authorities for the disclosure of stored computer data. Section 3 applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties.

4 Section 4 of this chapter consists of Article 10. It provides for procedures pertaining to emergency mutual assistance. Section 4 applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties.

5 Section 5 of this chapter consists of Articles 11 and 12. Section 5 applies where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties. The provisions of section 5 shall not apply where such treaty or arrangement exists, except as provided in Article 12, paragraph 7. However, the Parties concerned may mutually determine to apply the provisions of section 5 in lieu thereof, if the treaty or arrangement does not prohibit it.

6 Where, in accordance with the provisions of this Protocol, the requested Party is permitted to make co-operation conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

7 The provisions in this chapter do not restrict co-operation between Parties, or between Parties and service providers or other entities, through other applicable agreements, arrangements, practices, or domestic law.

Section 2 – Procedures enhancing direct co-operation with providers and entities in other
Parties

Article 6 – Request for domain name registration information

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, for the purposes of specific criminal investigations or proceedings, to issue a request to an entity providing domain name registration services in the territory of another Party for information in the entity's possession or control, for identifying or contacting the registrant of a domain name.

2 Each Party shall adopt such legislative and other measures as may be necessary to permit an entity in its territory to disclose such information in response to a request under paragraph 1, subject to reasonable conditions provided by domestic law.

3 The request under paragraph 1 shall include:

a the date on which the request was issued and the identity and contact details of the competent authority issuing the request;

b the domain name about which information is sought and a detailed list of the information sought, including the particular data elements;

c a statement that the request is issued pursuant to this Protocol, 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; and

d the time frame within which and the manner in which to disclose the information and any other special procedural instructions.

4 If acceptable to the entity, a Party may submit a request under paragraph 1 in electronic form. Appropriate levels of security and authentication may be required.

5 In the event of non-co-operation by an entity described in paragraph 1, a requesting Party may request that the entity give a reason why it is not disclosing the information sought. The requesting Party may seek consultation with the Party in which the entity is located, with a view to determining available measures to obtain the information.

6 Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, or at any other time, communicate to the Secretary General of the Council of Europe the authority designated for the purpose of consultation under paragraph 5.

7 The Secretary General of the Council of Europe shall set up and keep updated a register of authorities designated by the Parties under paragraph 6. Each Party shall ensure that the details that it has provided for the register are correct at all times.

Article 7 – Disclosure of subscriber information

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings.

2 a Each Party shall adopt such legislative and other measures as may be necessary for a service provider in its territory to disclose subscriber information in response to an order under paragraph 1.

b At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, a Party may – with respect to orders issued to service providers in its territory – make the following declaration: "The order under Article 7, paragraph 1, must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision".

3 The order under paragraph 1 shall specify:

- a the issuing authority and date issued;
- b a statement that the order is issued pursuant to this Protocol;
- c the name and address of the service provider(s) to be served;
- d the offence(s) that is/are the subject of the criminal investigation or proceeding;
- e the authority seeking the specific subscriber information, if not the issuing authority; and
- f a detailed description of the specific subscriber information sought.

4 The order under paragraph 1 shall be accompanied by the following supplemental information:

- a the domestic legal grounds that empower the authority to issue the order;
- b a reference to legal provisions and applicable penalties for the offence being investigated or prosecuted;
- c 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 respond;
- d the time frame within which and the manner in which to return the subscriber information;
- e whether preservation of the data has already been sought, including the date of preservation and any applicable reference number;
- f any special procedural instructions;

g if applicable, a statement that simultaneous notification has been made pursuant to paragraph 5; and

h any other information that may assist in obtaining disclosure of the subscriber information.

5 a A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, notify the Secretary General of the Council of Europe that, when an order is issued under paragraph 1 to a service provider in its territory, the Party requires, in every case or in identified circumstances, simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation or proceeding.

b Whether or not a Party requires notification under paragraph 5.a, it may require the service provider to consult the Party's authorities in identified circumstances prior to disclosure.

c The authorities notified under paragraph 5.a or consulted under paragraph 5.b may, without undue delay, instruct the service provider not to disclose the subscriber information if:

i disclosure may prejudice criminal investigations or proceedings in that Party; or

ii conditions or grounds for refusal would apply under Article 25, paragraph 4, and Article 27, paragraph 4, of the Convention had the subscriber information been sought through mutual assistance.

d The authorities notified under paragraph 5.a or consulted under paragraph 5.b:

i may request additional information from the authority referred to in paragraph 4.c for the purposes of applying paragraph 5.c and shall not disclose it to the service provider without that authority's consent; and

ii shall promptly inform the authority referred to in paragraph 4.c if the service provider has been instructed not to disclose the subscriber information and give the reasons for doing so.

e A Party shall designate a single authority to receive notification under paragraph 5.a and perform the actions described in paragraphs 5.b, 5.c and 5.d. The Party shall, at the time when notification to the Secretary General of the Council of Europe under paragraph 5.a is first given, communicate to the Secretary General the contact information of that authority.

f The Secretary General of the Council of Europe shall set up and keep updated a register of the authorities designated by the Parties pursuant to paragraph 5.e and whether and under what circumstances they require notification pursuant to paragraph 5.a. Each Party shall ensure that the details that it provides for the register are correct at all times.

6 If acceptable to the service provider, a Party may submit an order under paragraph 1 and supplemental information under paragraph 4 in electronic form. A Party may provide notification and additional information under paragraph 5 in electronic form. Appropriate levels of security and authentication may be required.

7 If a service provider informs the authority in paragraph 4.c that it will not disclose the subscriber information sought, or if it does not disclose subscriber information in response to the order under paragraph 1 within thirty days of receipt of the order or the timeframe stipulated in paragraph 4.d, whichever time period is longer, the competent authorities of the issuing Party may then seek to enforce the order only via Article 8 or other forms of mutual assistance. Parties may request that a service provider give a reason for refusing to disclose the subscriber information sought by the order.

8 A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that an issuing Party shall seek disclosure of subscriber information from the service provider before seeking it under Article 8, unless the issuing Party provides a reasonable explanation for not having done so.

9 At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may:

- a reserve the right not to apply this article; or
- b if disclosure of certain types of access numbers under this article would be inconsistent with the fundamental principles of its domestic legal system, reserve the right not to apply this article to such numbers.

Section 3 – Procedures enhancing international co-operation between authorities for the disclosure of stored computer data

Article 8 – Giving effect to orders from another Party for expedited production of subscriber information and traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted as part of a request to another Party for the purpose of compelling a service provider in the requested Party's territory to produce specified and stored

- a subscriber information, and
- b traffic data in that service provider's possession or control which is needed for the Party's specific criminal investigations or proceedings.

2 Each Party shall adopt such legislative and other measures as may be necessary to give effect to

an order under paragraph 1 submitted by a requesting Party.

3 In its request, the requesting Party shall submit the order under paragraph 1, the supporting information and any special procedural instructions to the requested Party.

- a The order shall specify:
 - i the issuing authority and the date the order was issued;
 - ii a statement that the order is submitted pursuant to this Protocol;

- iii the name and address of the service provider(s) to be served;
- iv the offence(s) that is/are the subject of the criminal investigation or proceeding;
- v the authority seeking the information or data, if not the issuing authority; and
- vi a detailed description of the specific information or data sought.

b The supporting information, provided for the purpose of assisting the requested Party to give effect to the order and which shall not be disclosed to the service provider without the consent of the requesting Party, shall specify:

- i the domestic legal grounds that empower the authority to issue the order;
- ii the legal provisions and applicable penalties for the offence(s) being investigated or prosecuted;
- iii the reason why the requesting Party believes that the service provider is in possession or control of the data;
- iv a summary of the facts related to the investigation or proceeding;
- v the relevance of the information or data to the investigation or proceeding;
- vi contact information of an authority or authorities that may provide further information;
- vii whether preservation of the information or data has already been sought, including the date of preservation and any applicable reference number; and
- viii whether the information or data have already been sought by other means, and, if so, in what manner.

c The requesting Party may request that the requested Party carry out special procedural instructions.

4 A Party may declare at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, that additional supporting information is required to give effect to orders under paragraph 1.

5 The requested Party shall accept requests in electronic form. It may require appropriate levels of security and authentication before accepting the request.

6 a The requested Party, from the date of receipt of all the information specified in paragraphs 3 and 4, shall make reasonable efforts to serve the service provider within forty-five days, if not sooner, and shall order a return of requested information or data no later than:

- i twenty days for subscriber information; and
- ii forty-five days for traffic data.

b The requested Party shall provide for the transmission of the produced information or data to the requesting Party without undue delay.

7 If the requested Party cannot comply with the instructions under paragraph 3.c in the manner requested, it shall promptly inform the requesting Party, and, if applicable, specify any conditions under which it could comply, following which the requesting Party shall determine whether the request should nevertheless be executed.

8 The requested Party may refuse to execute a request on the grounds established in Article 25, paragraph 4, or Article 27, paragraph 4, of the Convention or may impose conditions it considers necessary to permit execution of the request. The requested Party may postpone execution of requests for reasons established under Article 27, paragraph 5, of the Convention. The requested Party shall notify the requesting Party as soon as practicable of the refusal, conditions, or postponement. The requested Party shall also notify the requesting Party of other circumstances that are likely to delay execution of the request significantly. Article 28, paragraph 2.b, of the Convention shall apply to this article.

9 a If the requesting Party cannot comply with a condition imposed by the requested Party under paragraph 8, it shall promptly inform the requested Party. The requested Party shall then determine if the information or material should nevertheless be provided.

b If the requesting Party accepts the condition, it shall be bound by it. The requested Party that supplies information or material subject to such a condition may require the requesting Party to explain in relation to that condition the use made of such information or material.

10 Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe and keep up to date the contact information of the authorities designated:

- a to submit an order under this article; and
- b to receive an order under this article.

11 A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it requires that requests by other Parties under this article be submitted to it by the central authority of the requesting Party, or by such other authority as mutually determined between the Parties concerned.

12 The Secretary General of the Council of Europe shall set up and keep updated a register of authorities designated by the Parties under paragraph 10. Each Party shall ensure that the details that it has provided for the register are correct at all times.

13 At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may reserve the right not to apply this article to traffic data.

1 a Each Party shall adopt such legislative and other measures as may be necessary, in an emergency, for its point of contact for the 24/7 Network referenced in Article 35 of the Convention (“point of contact”) to transmit a request to and receive a request from a point of contact in another Party seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure of specified, stored computer data in that service provider’s possession or control, without a request for mutual assistance.

b A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it will not execute requests under paragraph 1.a seeking only the disclosure of subscriber information.

2 Each Party shall adopt such legislative and other measures as may be necessary to enable, pursuant to paragraph 1:

a its authorities to seek data from a service provider in its territory following a request under

paragraph 1;

b a service provider in its territory to disclose the requested data to its authorities in response to a request under paragraph 2.a; and

c its authorities to provide the requested data to the requesting Party.

3 The request under paragraph 1 shall specify:

a the competent authority seeking the data and date on which the request was issued;

b a statement that the request is issued pursuant to this Protocol;

c the name and address of the service provider(s) in possession or control of the data sought;

d the offence(s) that is/are the subject of the criminal investigation or proceeding and a reference to its legal provisions and applicable penalties;

e sufficient facts to demonstrate that there is an emergency and how the data sought relate to it;

f a detailed description of the data sought;

g any special procedural instructions; and

h any other information that may assist in obtaining disclosure of the requested data.

4 The requested Party shall accept a request in electronic form. A Party may also accept a request transmitted orally and may require confirmation in electronic form. It may require appropriate levels of security and authentication before accepting the request.

5 A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it requires requesting Parties, following the execution of the request, to submit the request and any supplemental information transmitted in support thereof, in a format and through such channel, which may include mutual assistance, as specified by the requested Party.

6 The requested Party shall inform the requesting Party of its determination on the request under paragraph 1 on a rapidly expedited basis and, if applicable, shall specify any conditions under which it would provide the data and any other forms of co-operation that may be available.

7 a If a requesting Party cannot comply with a condition imposed by the requested Party under paragraph 6, it shall promptly inform the requested Party. The requested Party shall then determine whether the information or material should nevertheless be provided. If the requesting Party accepts the condition, it shall be bound by it.

b The requested Party that supplies information or material subject to such a condition may require the requesting Party to explain in relation to that condition the use made of such information or material.

Section 4 – Procedures pertaining to emergency mutual assistance

Article 10 – Emergency mutual assistance

1 Each Party may seek mutual assistance on a rapidly expedited basis where it is of the view that an emergency exists. A request under this article shall include, in addition to the other contents required, a description of the facts that demonstrate that there is an emergency and how the assistance sought relates to it.

2 A requested Party shall accept such a request in electronic form. It may require appropriate levels of security and authentication before accepting the request.

3 The requested Party may seek, on a rapidly expedited basis, supplemental information in order to evaluate the request. The requesting Party shall provide such supplemental information on a rapidly expedited basis.

4 Once satisfied that an emergency exists and the other requirements for mutual assistance have been satisfied, the requested Party shall respond to the request on a rapidly expedited basis.

5 Each Party shall ensure that a person from its central authority or other authorities responsible for responding to mutual assistance requests is available on a twenty-four hour, seven-day-a-week basis for the purpose of responding to a request under this article.

6 The central authority or other authorities responsible for mutual assistance of the requesting and requested Parties may mutually determine that the results of the execution of a request under this article, or an advance copy thereof, may be provided to the requesting Party through a channel other than that used for the request.

7 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, Article 27, paragraphs 2.b and 3 to 8, and Article 28, paragraphs 2 to 4, of the Convention shall apply to this article.

8 Where such a treaty or arrangement exists, this article shall be supplemented by the provisions of

such treaty or arrangement unless the Parties concerned mutually determine to apply any or all of the provisions of the Convention referred to in paragraph 7 of this article, in lieu thereof.

9 Each Party may, at the time of signature of this Protocol or when depositing its instrument

of ratification, acceptance or approval, declare that requests may also be sent directly to its judicial authorities, or through the channels of the International Criminal Police Organization (INTERPOL) or to its 24/7 point of contact established under Article 35 of the Convention. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. Where a request is sent directly to a judicial authority of the requested Party and that authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform the requesting Party directly that it has done so.

Section 5 – Procedures pertaining to international co-operation in the absence of applicable
international agreements

Article 11 – Video conferencing

1 A requesting Party may request, and the requested Party may permit, testimony and statements to be taken from a witness or expert by video conference. The requesting Party and the requested Party shall consult in order to facilitate resolution of any issues that may arise with regard to the execution of the request, including, as applicable: which Party shall preside; the authorities and persons that shall be present; whether one or both Parties shall administer particular oaths, warnings or give instructions to the witness or expert; the manner of questioning the witness or expert; the manner in which the rights of the witness or expert shall be duly ensured; the treatment of claims of privilege or immunity; the treatment of objections to questions or responses; and whether one or both Parties shall provide translation, interpretation and transcription services.

2 a The central authorities of the requested and requesting Parties shall communicate directly with each other for the purposes of this article. A requested Party may accept a request in electronic form. It may require appropriate levels of security and authentication before accepting the request.

b The requested Party shall inform the requesting Party of the reasons for not executing or for delaying the execution of the request. Article 27, paragraph 8, of the Convention applies to this article. Without prejudice to any other condition a requested Party may impose in accordance with this article, Article 28, paragraphs 2 to 4, of the Convention apply to this article.

3 A requested Party providing assistance under this article shall endeavour to obtain the presence of the person whose testimony or statement is sought. Where appropriate the requested Party may, to the extent possible under its law, take the necessary measures to compel a witness or expert to appear in the requested Party at a set time and location.

4 The procedures relating to the conduct of the video conference specified by the requesting Party shall be followed, except where incompatible with the domestic law of the requested Party. In case of incompatibility, or to the extent that the procedure has not been specified by the requesting Party, the requested Party shall apply the procedure under its domestic law unless otherwise mutually determined by the requesting and requested Parties.

5 Without prejudice to any jurisdiction under the domestic law of the requesting Party, where in the course of the video conference, the witness or expert:

a makes an intentionally false statement when the requested Party has, in accordance with the domestic law of the requested Party, obliged such person to testify truthfully;

b refuses to testify when the requested Party has, in accordance with the domestic law of the requested Party, obliged such person to testify; or

c commits other misconduct that is prohibited by the domestic law of the requested Party in the course of such proceedings; the person shall be sanctionable in the requested Party in the same manner as if such act had been committed in the course of its domestic proceedings.

6 a Unless otherwise mutually determined between the requesting Party and the requested Party, the requested Party shall bear all costs related to the execution of a request under this article, except:

i the fees of an expert witness;

ii the costs of translation, interpretation and transcription; and

iii costs of an extraordinary nature.

b If the execution of a request would impose costs of an extraordinary nature, the requesting Party and the requested Party shall consult each other in order to determine the conditions under which the request may be executed.

7 Where mutually agreed upon by the requesting Party and the requested Party:

a the provisions of this article may be applied for the purposes of carrying out audio conferences;

b video conferencing technology may be used for purposes, or for hearings, other than those described in paragraph 1, including for the purposes of identifying persons or objects.

8 Where a requested Party chooses to permit the hearing of a suspect or accused person, it may require particular conditions and safeguards with respect to the taking of testimony or a statement from, or providing notifications or applying procedural measures to, such person.

Article 12 – Joint investigation teams and joint investigations

1 By mutual agreement, the competent authorities of two or more Parties may establish and operate a joint investigation team in their territories to facilitate criminal investigations or proceedings, where enhanced coordination is deemed to be of particular utility. The competent authorities shall be determined by the respective Parties concerned.

2 The procedures and conditions governing the operation of joint investigation teams, such as their specific purposes; composition; functions; duration and any extension periods; location; organisation; terms of gathering, transmitting and using information or evidence; terms of confidentiality; and terms for the involvement of the participating authorities of a Party in investigative activities taking place in another Party's territory, shall be as agreed between those competent authorities.

3 A Party may declare at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval that its central authority must be a signatory to or otherwise concur in the agreement establishing the team.

4 Those competent and participating authorities shall communicate directly, except that Parties may mutually determine other appropriate channels of communication where exceptional circumstances require more central coordination.

5 Where investigative measures need to be taken in the territory of one of the Parties concerned, participating authorities from that Party may request their own authorities to take those measures without the other Parties having to submit a request for mutual assistance. Those measures shall be carried out by that Party's authorities in its territory under the conditions that apply under domestic law in a national investigation.

6 Use of information or evidence provided by the participating authorities of one Party to participating authorities of other Parties concerned may be refused or restricted in the manner set forth in the agreement described in paragraphs 1 and 2. If that agreement does not set forth terms for refusing or restricting use, the Parties may use the information or evidence provided:

a for the purposes for which the agreement has been entered into;

b for detecting, investigating and prosecuting criminal offences other than those for which the agreement was entered into, subject to the prior consent of the authorities providing the information or evidence. However, consent shall not be required where fundamental legal principles of the Party using the information or evidence require that it disclose the information or evidence to protect the rights of an accused person in criminal proceedings. In that case, those authorities shall notify the authorities that provided the information or evidence without undue delay; or

c to prevent an emergency. In that case, the participating authorities that received the information or evidence shall notify without undue delay the participating authorities that provided the information or evidence, unless mutually determined otherwise.

7 In the absence of an agreement described in paragraphs 1 and 2, joint investigations may be undertaken under mutually agreed terms on a case-by-case basis. This paragraph applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned.

Chapter III – Conditions and safeguards

Article 13 – Conditions and safeguards

In accordance with Article 15 of the Convention, each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Protocol are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties.

Article 14 – Protection of personal data

1 Scope

a Except as otherwise provided in paragraphs 1.b and c, each Party shall process the personal data that it receives under this Protocol in accordance with paragraphs 2 to 15 of this article.

b If, at the time of receipt of personal data under this Protocol, both the transferring Party and the receiving Party are mutually 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, and which provides that the processing of personal data under that agreement complies with the requirements of the data protection legislation of the Parties concerned, the terms of such agreement shall apply, for the measures falling within the scope of such agreement, to personal data received under this Protocol in lieu of paragraphs 2 to 15, unless otherwise agreed between the Parties concerned.

c If the transferring Party and the receiving Party are not mutually bound under an agreement described in paragraph 1.b, they may mutually determine that the transfer of personal data under this Protocol may take place on the basis of other agreements or arrangements between the Parties concerned in lieu of paragraphs 2 to 15.

d Each Party shall consider that the processing of personal data pursuant to paragraphs 1.a and 1.b meets the requirements of its personal data protection legal framework for international transfers of personal data, and no further authorisation for transfer shall be required under that legal framework. A Party may only refuse or prevent data transfers to another Party under this Protocol for reasons of data protection under the conditions set out in paragraph 15 when paragraph 1.a applies; or under the terms of an agreement or arrangement referred to in paragraphs 1.b or c, when one of those paragraphs applies.

e Nothing in this article shall prevent a Party from applying stronger safeguards to the processing by its own authorities of personal data received under this Protocol.

2 Purpose and use

a The Party that has received personal data shall process them for the purposes described in Article 2. It shall not further process the personal data for an incompatible purpose, and it shall not further process the data when this is not permitted under its domestic legal framework. This article shall not prejudice the ability of the transferring Party to impose additional conditions pursuant to this Protocol in a specific case, however, such conditions shall not include generic data protection conditions.

b The receiving Party shall ensure under its domestic legal framework that personal data sought and processed are relevant to and not excessive in relation to the purposes of such processing.

3 Quality and integrity

Each Party shall take reasonable steps to ensure that personal data are maintained with such accuracy and completeness and are as up to date as is necessary and appropriate for the lawful processing of the personal data, having regard to the purposes for which they are processed.

4 Sensitive data

Processing by a Party of personal data revealing racial or ethnic origin, political opinions or religious or other beliefs, or trade union membership; genetic data; biometric data considered sensitive in view of the risks involved; or personal data concerning health or sexual life; shall only take place under appropriate safeguards to guard against the risk of unwarranted prejudicial impact from the use of such data, in particular against unlawful discrimination.

5 Retention periods

Each Party shall retain the personal data only for as long as necessary and appropriate in view of the purposes of processing the data pursuant to paragraph 2. In order to meet this obligation, it shall provide in its domestic legal framework for specific retention periods or periodic review of the need for further retention of the data.

6 Automated decisions

Decisions producing a significant adverse effect concerning the relevant interests of the individual to whom the personal data relate may not be based solely on automated processing of personal data, unless authorised under domestic law and with appropriate safeguards that include the possibility to obtain human intervention.

7 Data security and security incidents

a Each Party shall ensure that it has in place appropriate technological, physical and organisational measures for the protection of personal data, in particular against loss or accidental or unauthorised access, disclosure, alteration or destruction (“security incident”).

b Upon discovery of a security incident in which there is a significant risk of physical or nonphysical harm to individuals or to the other Party, the receiving Party shall promptly assess the likelihood and scale thereof and shall promptly take appropriate action to mitigate such harm. Such action shall include notification to the transferring authority or, for purposes of Chapter II, section 2, the authority or authorities designated pursuant to paragraph 7.c. However, notification may include appropriate restrictions as to the further transmission of the notification; it may be delayed or omitted when such notification may endanger national security, or delayed when such notification may endanger measures to protect public safety. Such action shall also include notification to the individual concerned, unless the Party has taken appropriate measures so that there is no longer a significant risk. Notification to the individual may be delayed or omitted under the conditions set out in paragraph 12.a.i. The notified Party may request consultation and additional information concerning the incident and the response thereto.

c Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe the authority or authorities to be notified under paragraph 7.b for the purposes of Chapter II, section 2; the information provided may subsequently be modified.

8 Maintaining records Each Party shall maintain records or have other appropriate means to demonstrate how an individual’s personal data are accessed, used and disclosed in a specific case.

9 Onward sharing within a Party

a When an authority of a Party provides personal data received initially under this Protocol to another authority of that Party, that other authority shall process it in accordance with this article, subject to paragraph 9.b.

b Notwithstanding paragraph 9.a, a Party that has made a reservation under Article 17 may provide personal data it has received to its constituent States or similar territorial entities provided the Party has in place measures in order that the receiving authorities continue to effectively protect the data by providing for a level of protection of the data comparable to that afforded by this article.

c In case of indications of improper implementation of this paragraph, the transferring Party may request consultation and relevant information about those indications.

10 Onward transfer to another State or international organisation

a The receiving Party may transfer the personal data to another State or international organisation only with the prior authorisation of the transferring authority or, for purposes of Chapter II, section 2, the authority or authorities designated pursuant to paragraph 10.b.

b Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe the authority or authorities to provide authorisation for purposes of Chapter II, section 2; the information provided may subsequently be modified.

11 Transparency and notice

a Each Party shall provide notice through the publication of general notices, or through personal notice to the individual whose personal data have been collected, with regard to:

- i the legal basis for and the purpose(s) of processing;
- ii any retention or review periods pursuant to paragraph 5, as applicable;
- iii recipients or categories of recipients to whom such data are disclosed;

and

- iv access, rectification and redress available.

b A Party may subject any personal notice requirement to reasonable restrictions under its domestic legal framework pursuant to the conditions set forth in paragraph 12.a.i.

c Where the transferring Party's domestic legal framework requires giving personal notice to the individual whose data have been provided to another Party, the transferring Party shall take measures so that the other Party is informed at the time of transfer regarding this requirement and appropriate contact information. The personal notice shall not be given if the other Party has requested that the provision of the data be kept confidential, where the conditions for restrictions as set out in paragraph 12.a.i apply. Once these restrictions no longer apply and the personal notice can be provided, the other Party shall take measures so that the transferring Party is informed. If it has not yet been informed, the transferring Party is entitled to make requests to the receiving Party which will inform the transferring Party whether to maintain the restriction.

12 Access and rectification

a Each Party shall ensure that any individual, whose personal data have been received under this Protocol is entitled to seek and obtain, in accordance with processes established in its domestic legal framework and without undue delay:

i a written or electronic copy of the documentation kept on that individual containing the individual's personal data and available information indicating the legal basis for and purposes of the processing, retention periods and recipients or categories of recipients of the data ("access"), as well as information regarding available options for redress; provided that access in a particular case may be subject to the application of proportionate restrictions permitted under its domestic legal framework, needed, at the time of adjudication, to protect the rights and freedoms of others or important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned;

ii rectification when the individual's personal data are inaccurate or have been improperly processed; rectification shall include – as appropriate and reasonable considering the grounds for rectification and the particular context of processing – correction, supplementation, erasure or anonymisation, restriction of processing, or blocking.

b If access or rectification is denied or restricted, the Party shall provide to the individual, in written form which may be provided electronically, without undue delay, a response informing that individual of the denial or restriction. It shall provide the grounds for such denial or restriction and provide information about available options for redress. Any expense incurred in obtaining access should be limited to what is reasonable and not excessive.

13 Judicial and non-judicial remedies

Each Party shall have in place effective judicial and non-judicial remedies to provide redress for violations of this article.

14 Oversight

Each Party shall have in place one or more public authorities that exercise, alone or cumulatively, independent and effective oversight functions and powers with respect to the measures set forth in this article. The functions and powers of these authorities acting alone or cumulatively shall include investigation powers, the power to act upon complaints and the ability to take corrective action.

15 Consultation and suspension

A Party may suspend the transfer of personal data to another Party if it has substantial evidence that the other Party is in systematic or material breach of the terms of this article or that a material breach is imminent. It shall not suspend transfers without reasonable notice, and not until after the Parties concerned have engaged in a reasonable period of consultation without reaching a resolution. However, a Party may provisionally suspend transfers in the event of a systematic or material breach that poses a significant and imminent risk to the life or safety of, or substantial reputational or monetary harm to, a natural person, in which case it shall notify and commence consultations with the other Party immediately thereafter. If the consultation has not led to a resolution, the other Party may reciprocally suspend transfers if it has substantial evidence that suspension by the suspending Party was contrary to the terms of this paragraph. The suspending Party shall lift the suspension as soon as the breach justifying the suspension has been remedied; any

reciprocal suspension shall be lifted at that time. Any personal data transferred prior to suspension shall continue to be treated in accordance with this Protocol.

Chapter IV – Final provisions

Article 15 – Effects of this Protocol

- 1 a Article 39, paragraph 2, of the Convention shall apply to this Protocol.
 b With respect to Parties that are members of the European Union, those Parties may, in their mutual relations, apply European Union law governing the matters dealt with in this Protocol.
 c Paragraph 1.b does not affect the full application of this Protocol between Parties that are members of the European Union and other Parties.
- 2 Article 39, paragraph 3, of the Convention shall apply to this Protocol.

Article 16 – Signature and entry into force

- 1 This Protocol shall be open for signature by Parties to the Convention, which may express their consent to be bound by either:
 - a signature without reservation as to ratification, acceptance or approval; or
 - b signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.
- 2 Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
- 3 This Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five Parties to the Convention have expressed their consent to be bound by this Protocol, in accordance with the provisions of paragraphs 1 and 2 of this article.
- 4 In respect of any Party to the Convention which subsequently expresses its consent to be bound by this Protocol, this Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date on which the Party has expressed its consent to be bound by this Protocol, in accordance with the provisions of paragraphs 1 and 2 of this article.

Article 17 – Federal clause

- 1 A federal State may reserve the right to assume obligations under this Protocol consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities, provided that:
 - a this Protocol shall apply to the central government of the federal State;

b such a reservation shall not affect obligations to provide for the co-operation sought by other Parties in accordance with the provisions of Chapter II; and

c the provisions of Article 13 shall apply to the federal State's constituent States or other similar territorial entities.

2 Another Party may prevent authorities, providers or entities in its territory from co-operating in response to a request or order submitted directly by the constituent State or other similar territorial entity of a federal State that has made a reservation under paragraph 1, unless that federal State notifies the Secretary General of the Council of Europe that a constituent State or other similar territorial entity applies the obligations of this Protocol applicable to that federal State. The Secretary General of the Council of Europe shall set up and keep updated a register of such notifications.

3 Another Party shall not prevent authorities, providers, or entities in its territory from co-operating with a constituent State or other similar territorial entity on the grounds of a reservation under paragraph 1, if an order or request has been submitted via the central government or a joint investigation team agreement under Article 12 is entered into with the participation of the central government. In such situations, the central government shall provide for the fulfilment of the applicable obligations of this Protocol, provided that, with respect to the protection of personal data provided to constituent States or similar territorial entities, only the terms of Article 14, paragraph 9, or, where applicable, the terms of an agreement or arrangement described in Article 14, paragraphs 1.b or 1.c, shall apply.

4 With regard to the provisions of this Protocol, the application of which comes under the jurisdiction of constituent States or other similar territorial entities that are not obliged by the constitutional system of the federation to take legislative measures, the central government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 18 – Territorial application

1 This Protocol shall apply to the territory or territories specified in a declaration made by a Party under Article 38, paragraphs 1 or 2, of the Convention to the extent that such declaration has not been withdrawn under Article 38, paragraph 3.

2 A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that this Protocol shall not apply to one or more territories specified in the Party's declaration under Article 38, paragraphs 1 and/or 2, of the Convention.

3 A declaration under paragraph 2 of this article may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 19 – Reservations and declarations

1 By a written notification addressed to the Secretary General of the Council of Europe, any Party to the Convention may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it avails itself of the reservation(s) provided for in Article 7, paragraphs 9.a and 9.b, Article 8, paragraph 13, and Article 17 of this Protocol. No other reservations may be made.

2 By a written notification addressed to the Secretary General of the Council of Europe, any Party to the Convention may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, make the declaration(s) identified in Article 7, paragraphs 2.b and 8; Article 8, paragraph 11; Article 9, paragraphs 1.b and 5; Article 10, paragraph 9; Article 12, paragraph 3; and Article 18, paragraph 2, of this Protocol.

3 By a written notification addressed to the Secretary General of the Council of Europe, any Party to the Convention shall make any declaration(s), notifications or communications identified in Article 7, paragraphs 5.a and 5.e; Article 8, paragraphs 4, 10.a and 10.b; Article 14, paragraphs 7.c and 10.b; and Article 17, paragraph 2, of this Protocol according to the terms specified therein.

Article 20 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 19, paragraph 1, shall withdraw such reservation, in whole or in part, as soon as circumstances so permit. Such withdrawal shall take effect on the date of receipt of a notification addressed to the Secretary General of the Council of Europe. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on this later date.

2 The Secretary General of the Council of Europe may periodically enquire of Parties that have made one or more reservations in accordance with Article 19, paragraph 1, as to the prospects for withdrawing such reservation(s).

Article 21 – Amendments

1 Amendments to this Protocol may be proposed by any Party to this Protocol and shall be communicated by the Secretary General of the Council of Europe, to the member States of the Council of Europe and to the Parties and signatories to the Convention as well as to any State which has been invited to accede to the Convention.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the Parties to the Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 shall be forwarded to the Parties to this Protocol for acceptance.

5 Any amendment adopted in accordance with paragraph 3 shall come into force on the thirtieth day after all Parties to this Protocol have informed the Secretary General of their acceptance thereof.

Article 22 – Settlement of disputes

Article 45 of the Convention shall apply to this Protocol.

Article 23 – Consultations of the Parties and assessment of implementation

1 Article 46 of the Convention shall apply to this Protocol.

2 Parties shall periodically assess the effective use and implementation of the provisions of this Protocol. Article 2 of the Cybercrime Convention Committee Rules of Procedure as revised on 16 October 2020 shall apply *mutatis mutandis*. The Parties shall initially review and may modify by consensus the procedures of that article as they apply to this Protocol five years after the entry into force of this Protocol.

3 The review of Article 14 shall commence once ten Parties to the Convention have expressed their consent to be bound by this Protocol.

Article 24 – Denunciation

1 Any Party may, at any time, denounce this Protocol by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

3 Denunciation of the Convention by a Party to this Protocol constitutes denunciation of this Protocol.

4 Information or evidence transferred prior to the effective date of denunciation shall continue to be treated in accordance with this Protocol.

Article 25 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the Parties and signatories to the Convention, and any State which has been invited to accede to the Convention of:

- a any signature;
- b the deposit of any instrument of ratification, acceptance or approval;

c any date of entry into force of this Protocol in accordance with Article 16, paragraphs 3 and 4;

d any declarations or reservations made in accordance with Article 19 or withdrawal of reservations made in accordance with Article 20;

e any other act, notification or communication relating to this Protocol.

In witness whereof the undersigned, being duly authorised thereto, have signed this Protocol.

Done at Strasbourg on the 12th day of May 2022, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the Parties and Signatories to the Convention, and to any State which has been invited to accede to the Convention.

DRUGI DODATNI PROTOKOL UZ KONVENCIJU O RAČUNARSKOM KRIMINALU O UNAPRIJEĐENOJ SARADNJI I OTKRIVANJU ELEKTRONSKIH DOKAZA

Preambula

Države članice Savjeta Evrope i ostale države Strane Konvencije o računarskom kriminalu (ETS br. 185, u daljem tekstu: Konvencija), otvorene za potpisivanje u Budimpešti dana 23. novembra 2001. godine, potpisnice ovog protokola, imajući u vidu domašaj i uticaj Konvencije u svim regionima svijeta;

Podsjećajući da je Konvencija već dopunjena Dodatnim protokolom o inkriminaciji akata rasizma i ksenofobije učinjenih putem računarskih sistema (ETS br. 189), otvorenim za potpisivanje u Strazburu 28. januara 2003. godine (u daljem tekstu: Prvi protokol), za Strane tog Protokola;

Uzimajući u obzir postojeće ugovore Savjeta Evrope o saradnji u krivičnim stvarima, kao i druge sporazume i dogovore o saradnji u krivičnim stvarima između Strana Konvencije;

Uzimajući u obzir i Konvenciju za zaštitu lica u odnosu na automatsku obradu ličnih podataka (ETS br. 108) kako je izmijenjena njenim Protokolom o izmjeni (CETS br. 223), otvorenim za potpisivanje u Strazburu 10. oktobra 2018. godine, kojoj svaka država može biti pozvana da pristupi;

Prepoznajući sve veću upotrebu informacione i komunikacione tehnologije, uključujući internet usluge, i rastući računarski kriminal koji predstavlja prijetnju demokratiji i vladavini prava i koji mnoge države smatraju i prijetnjom ljudskim pravima;

Prepoznajući i sve veći broj žrtava računarskog kriminala i važnost ostvarivanja pravde za te žrtve;

Podsjećajući na to da su vlade odgovorne da zaštite društvo i pojedince od kriminala ne samo van interneta nego i na internetu, između ostalog i djelotvornim krivičnim istragama i gonjenjem;

Svjesne da se dokazi o bilo kom krivičnom djelu sve više pohranjuju u elektronskom obliku na računarskim sistemima u stranim, višestrukim ili nepoznatim jurisdikcijama, i uvjerene da su potrebne dodatne mjere da bi se zakonito pribavili takvi dokazi kako bi se omogućio djelotvoran odgovor krivičnog pravosuđa i podržala vladavina prava;

Prepoznajući potrebu za povećanom i efikasnijom saradnjom država i privatnog sektora i da je u tom kontekstu potrebna veća jasnoća odnosno pravna sigurnost za pružaoce usluga i druge subjekte u pogledu okolnosti u kojima mogu da odgovore na direktne zahtjeve organa krivičnog pravosuđa drugih Strana za otkrivanje elektronskih podataka;

Nastojeći stoga da dodatno unaprijede saradnju u oblasti računarskog kriminala i prikupljanja dokaza u elektronskoj formi za bilo koje krivično djelo za potrebe konkretnih krivičnih istraga ili postupaka putem dodatnih alata koji se odnose na efikasniju uzajamnu pomoć i druge oblike saradnje između nadležnih organa, saradnju u hitnim situacijama i direktnu saradnju nadležnih organa i pružalaca usluga i drugih subjekata koji posjeduju ili kontrolišu relevantne informacije;

Uvjerene da su za djelotvornu prekograničnu saradnju za potrebe krivičnog pravosuđa, između ostalog i između javnog i privatnog sektora, korisni djelotvorni uslovi i mjere za zaštitu ljudskih prava i osnovnih sloboda;

Prepoznajući da se prikupljanje elektronskih dokaza za krivične istrage često odnosi na lične podatke i prepoznajući da je u mnogim Stranama propisano da se štite privatnost i lični podaci kako bi ispunile svoje ustavne i međunarodne obaveze; i

Imajući u vidu potrebu da se obezbijedi da djelotvorne krivičnopravne mjere u vezi sa računarskim kriminalom i prikupljanjem dokaza u elektronskoj formi podliježu uslovima i zaštitnim mjerama koje obezbjeđuju odgovarajuću zaštitu ljudskih prava i osnovnih sloboda, uključujući prava koja proizilaze iz obaveza koje su države preuzele u okviru važećih međunarodnih dokumenata o ljudskim pravima, kao što su Konvencija za zaštitu ljudskih prava i osnovnih sloboda iz 1950. godine (ETS br. 5) Savjeta Evrope, Međunarodni pakt o građanskim i političkim pravima Ujedinjenih nacija iz 1966. godine, Afrička povelja o ljudskim pravima i pravima naroda iz 1981. godine, Američka konvencija o ljudskim pravima iz 1969. godine i drugi međunarodni ugovori o ljudskim pravima;

Sporazumjele su se o sljedećem:

Poglavlje I

Opšte odredbe

Svrha

Član 1

Svrha ovog protokola je da dopuni:

- a) Konvenciju za Strane ovog protokola; i
- b) Prvi protokol za Strane ovog protokola koje su ujedno Strane Prvog protokola.

Područje primjene

Član 2

1. Ako u ovom protokolu nije navedeno drukčije, mjere opisane u ovom protokolu primjenjuju se:

a) između Strana Konvencije koje su Strane ovog protokola, na konkretne krivične istrage ili postupke koji se odnose na krivična djela povezana sa računarskim sistemima i podacima, i na prikupljanje dokaza o krivičnom djelu u elektronskom obliku; i

b) između Strana Prvog protokola koje su Strane ovog protokola, na konkretne krivične istrage ili postupke koji se odnose na krivična djela utvrđena u skladu sa Prvim protokolom.

2. Svaka Strana donosi zakonodavne i druge mjere koje su potrebne za izvršavanje obaveza utvrđenih ovim protokolom.

Značenja izraza

Član 3

1. Značenja izraza iz člana 1 i člana 18 stav 3 Konvencije primjenjuju se na ovaj protokol.

2. U smislu ovog protokola primjenjuju se sljedeća dodatna značenja izraza:

a) „centralni organ” je organ ili organi određeni ugovorom ili dogovorom o uzajamnoj pomoći na osnovu jednoobraznog ili recipročnog zakonodavstva koje je na snazi između predmetnih Strana ili, u odsustvu toga, organ ili organi koje je Strana odredila u skladu sa članom 27 stav 2 tačka a Konvencije;

b) „nadležni organ” je pravosudni, upravni ili drugi organ za sprovođenje zakona koji je domaćim zakonom ovlašćen da naloži, odobri ili preduzme izvršenje mjera na osnovu ovog protokola radi prikupljanja ili podnošenja dokaza u vezi sa konkretnim krivičnim istragama ili postupcima;

c) „hitna situacija” je situacija u kojoj postoji znatna i neposredna opasnost po život ili bezbjednost bilo kojeg fizičkog lica;

d) „lični podaci” su svaka informacija koja se odnosi na identifikovano fizičko lice ili fizičko lice koje se može identifikovati;

e) „Strana prenosilac” je Strana koja prenosi podatke kao odgovor na zahtjev ili kao dio zajedničkog istražnog tima ili, u smislu odjeljka 2 Poglavlja II, Strana na čijoj se

teritoriji nalazi pružalac usluge prenosa ili subjekt koji pruža usluge registracije naziva domena.

Jezik

Član 4

1 Zahtjevi, nalozi i prateće informacije dostavljene Strani moraju biti na jeziku prihvatljivom zamoljenoj Strani ili Strani koja je obaviještena u skladu sa članom 7 stav 5 ili se uz njih prilaže prevod na taj jezik.

2 Nalozi na osnovu člana 7 i zahtjevi na osnovu člana 6, kao i sve prateće informacije:

a) dostavljaju se na jeziku druge Strane na kojem ih pružalac usluga ili subjekt prihvata u uporedivom domaćem postupku;

b) dostavljaju se na drugom jeziku koji je prihvatljiv pružaocu usluga ili subjektu;
ili

c) praćeni su prevodom na jedan od jezika iz stava 2 tač. a ili b.

Poglavlje II

Mjere za unaprijeđenje saradnje

Odjeljak 1

Opšta načela koja se primjenjuju na Poglavlje II

Član 5

1. Strane sarađuju u skladu sa odredbama ovog poglavlja u najvećoj mogućoj mjeri.

2. Odjeljak 2 ovog poglavlja sastoji se od čl. 6 i 7. Njime su predviđeni postupci kojima se unapređuje neposredna saradnja sa pružaocima i subjektima na teritoriji druge Strane. Odjeljak 2 primjenjuje se nezavisno od toga da li postoji ugovor ili dogovor o uzajamnoj pomoći na osnovu jednoobraznog ili recipročnog zakonodavstva koje je na snazi između predmetnih Strana.

3. Odjeljak 3 ovog poglavlja sastoji se od čl. 8 i 9. Njime su predviđeni postupci za unapređenje međunarodne saradnje između organa u otkrivanju pohranjenih računarskih podataka. Odjeljak 3 primjenjuje se nezavisno od toga da li postoji ugovor ili dogovor o uzajamnoj pomoći na osnovu jednoobraznog ili recipročnog zakonodavstva koje je na snazi između Strane molilje i zamoljene Strane.

4. Odjeljak 4 ovog poglavlja sastoji se od člana 10. Njime su predviđeni postupci koji se odnose na uzajamnu pomoć u hitnim situacijama. Odjeljak 4 primjenjuje se nezavisno od toga da li postoji ugovor ili dogovor o uzajamnoj pomoći na osnovu jednoobraznog ili recipročnog zakonodavstva koje je na snazi između Strane molilje i zamoljene Strane.

5. Odjeljak 5 ovog poglavlja sastoji se od čl. 11 i 12. Odjeljak 5 primjenjuje se kada ne postoji ugovor ili dogovor o uzajamnoj pomoći na osnovu jednoobraznog ili recipročnog zakonodavstva koje je na snazi između Strane molilje i zamoljene Strane. Odredbe Odjeljka 5 ne primjenjuju se ako takav ugovor ili dogovor postoji, osim ako je to predviđeno članom 12 stav 7. Međutim, predmetne Strane mogu uzajamno da odluče da se umjesto toga primjenjuju odredbe Odjeljka 5 ako to ugovorom ili dogovorom nije zabranjeno.

6. Ako je, u skladu sa odredbama ovog protokola, zamoljenoj Strani dozvoljeno da uslovi saradnju postojanjem dvostruke inkriminacije, taj uslov smatra se ispunjenim bez obzira na to da li je njenim zakonima to krivično djelo stavljeno u istu kategoriju krivičnog djela ili se u nazivu krivičnog djela koristi ista terminologija kao i u Strani molilji ako je postupanje na kojem se zasniva krivično djelo za koje se traži uzajamna pomoć krivično djelo po njenim zakonima.

7. Odredbama ovog poglavlja ne ograničava se saradnja između Strana, ili između Strana i pružalaca usluga ili drugih subjekata, u okviru drugih važećih sporazuma, dogovora, praksi ili domaćeg prava.

Odjeljak 2

Postupci kojima se unaprijeđuje neposredna saradnja sa pružaocima i subjektima u drugim Stranama

Zahtjev za informacijama o registraciji naziva domena

Član 6

1. Svaka Strana donosi zakonodavne i druge mjere koje su potrebne da se njeni nadležni organi ovlaste, za potrebe konkretnih krivičnih istraga ili postupaka, za izdavanje zahtjeva subjektu koji pruža usluge registracije naziva domena na teritoriji druge Strane za informacijama koje taj subjekt posjeduje ili kontroliše, radi identifikacije ili kontaktiranja registranta naziva domena.

2. Svaka Strana donosi zakonodavne i druge mjere koje su potrebne da se subjektu na njenoj teritoriji omogući otkrivanje informacija kao odgovor na zahtjev iz stava 1, uz poštovanje opravdanih uslova predviđenih domaćim pravom.

3. Zahtjev iz stava 1 uključuje:

a) datum izdavanja zahtjeva i identitet i kontakt podatke nadležnog organa koji je izdao zahtjev;

b) naziv domena o kojem se traže informacije i detaljnu listu traženih informacija, uključujući i određene elemente podataka;

c) izjavu da se zahtjev izdaje u skladu sa ovim protokolom, da potreba za informacijama proizilazi iz njihove važnosti za konkretnu krivičnu istragu ili postupak i da će se informacije upotrebljavati samo za tu konkretnu krivičnu istragu ili postupak; i

d) vremenski okvir i način na koji treba otkriti informacije i sva druga posebna procesna uputstva.

4. Ako je to prihvatljivo subjektu, Strana može podnijeti zahtjev iz stava 1 u elektronskom obliku. Mogu se zahtijevati odgovarajući nivoi sigurnosti i autentifikacije.

5. U slučaju izostanka saradnje subjekta opisanog u stavu 1, Strana molilja može zahtijevati da subjekt navede razlog zbog kojeg ne otkriva tražene informacije. Strana molilja može zatražiti konsultacije sa Stranom u kojoj se subjekt nalazi, u cilju utvrđivanja dostupnih mjera za pribavljanje informacija.

6. Svaka Strana u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, ili u bilo kojem drugom trenutku, obavještava generalnog sekretara Savjeta Evrope o organu određenom za potrebe konsultacija u skladu sa stavom 5.

7. Generalni sekretar Savjeta Evrope uspostavlja i redovno ažurira registar organa koje su Strane odredile u skladu sa stavom 6. Svaka Strana dužna je da obezbijedi da su podaci koje je dostavila za registar u svakom trenutku tačni.

Otkrivanje podataka o pretplatnicima

Član 7

1. Svaka Strana donosi zakonodavne i druge mjere koje su potrebne da se njeni nadležni organi ovlaste za izdavanje naloga koji se dostavlja direktno pružaocu usluga na teritoriji druge Strane kako bi se pribavilo otkrivanje određenih pohranjenih podataka o pretplatnicima koje posjeduje ili kontroliše taj pružalac usluga, ako su podaci o pretplatnicima potrebni za konkretne krivične istrage ili postupke Strane izdavaoca.

2. a) Svaka Strana donosi zakonodavne i druge mjere koje su potrebne da bi pružalac usluga na njenoj teritoriji otkrio podatke o pretplatnicima kao odgovor na nalog iz stava 1.

b) U trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, Strana može – u odnosu na naloge izdate pružiocima usluga na njenoj teritoriji – dati sljedeću izjavu: „Nalog iz člana 7 stav 1 mora biti izdat od strane ili pod nadzorom tužioca ili drugog pravosudnog organa ili se mora izdati na neki drugi način pod nezavisnim nadzorom“.

3) U nalogu iz stava 1 navode se:

- a) organ izdavalac i datum izdavanja;
- b) izjava da je nalog izdat u skladu sa ovim protokolom;
- c) naziv i adresa pružaoca odnosno pružalaca usluga kojima treba uručiti nalog;
- d) krivično djelo odnosno djela koja su predmet krivične istrage ili postupka;
- e) organ koji traži konkretne podatke o pretplatnicima, ako nije riječ o organu izdavaocu; i

- f) detaljni opis konkretnih podataka o pretplatnicima koji se traže.
- 4) Uz nalog iz stava 1 prilažu se sljedeće dopunske informacije:
- a) domaći pravni osnov na osnovu koga je organ ovlašten za izdavanje naloga;
 - b) upućivanje na zakonske odredbe i propisane kazne za krivično djelo koje se istražuje ili za koje se krivično goni;
 - c) kontakt podaci organa kojem pružalac usluga treba da pošalje podatke o pretplatnicima, od kojeg može da zahtjeva dodatne informacije ili kojem na neki drugi način treba da odgovori;
 - d) vremenski okvir i način na koji treba poslati podatke o pretplatnicima;
 - e) da li je već zatraženo čuvanje podataka, uključujući datum čuvanja i svaki primjenjivi referentni broj;
 - f) sva posebna procesna uputstva;
 - g) ako je primjenjivo, izjava da je istovremeno poslato obavještenje u skladu sa stavom 5; i
 - h) sve druge informacije koje mogu pomoći u pribavljanju otkrivanja podataka o pretplatnicima.
5. a) Strana može, u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, ili u bilo kojem drugom trenutku, obavijestiti generalnog sekretara Savjeta Evrope da, kada se u skladu sa stavom 1 izdaje nalog pružaocu usluga na njenoj teritoriji, Strana zahtijeva, u svakom slučaju ili u određenim okolnostima, istovremeno obavještenje o nalogu, dopunske informacije i sažetak činjenica koje se odnose na istragu ili postupak.
- b) Bez obzira na to da li Strana zahtijeva obavještenje u skladu sa stavom 5 tačka a, može od pružaoca usluga zatražiti da se u određenim okolnostima prije otkrivanja konsultuje sa njenim nadležnim organima.
- c) Organi koji su obaviješteni u skladu sa stavom 5 tačka a ili koji su konsultovani u skladu sa stavom 5 tačka b mogu bez nepotrebnog odlaganja naložiti pružaocu usluga da ne otkriva podatke o pretplatnicima ako:
- i otkrivanje bi moglo ugroziti krivične istrage ili postupke u toj Strani; ili
 - ii uslovi ili razlozi za odbijanje bi se primjenjivali u skladu sa članom 25 stav 4 i članom 27 stav 4 Konvencije da su podaci o pretplatnicima bili traženi u okviru uzajamne pomoći.
- d) Organi koji su obaviješteni u skladu sa stavom 5 tačka a ili koji su konsultovani u skladu sa stavom 5 tačka b:
- i mogu zahtijevati dodatne informacije od organa iz stava 4 tačka c za potrebe primjene stava 5 tačka c i ne smiju ih otkriti pružaocu usluga bez saglasnosti tog organa; i

ii dužni su da odmah obavijeste organ iz stava 4 tačka c ako je pružaocu usluga naloženo da ne otkriva podatke o pretplatnicima i da navedu razloge za to.

e) Strana određuje jedan organ za primanje obavještenja iz stava 5 tačka a i vršenje radnji opisanih u stavu 5 tač. b, c i d. U trenutku prvog obavještanja generalnog sekretara Savjeta Evrope u skladu sa stavom 5 tačka a, Strana saopštava generalnom sekretaru kontakt podatke tog organa.

f) Generalni sekretar Savjeta Evrope uspostavlja i redovno ažurira registar organa koje su Strane odredile u skladu sa stavom 5 tačka e i u njemu navodi da li i u kojim okolnostima zahtijevaju obavještenje u skladu sa stavom 5 tačka a. Svaka Strana dužna je da obezbijedi da su podaci koje dostavlja za registar u svakom trenutku tačni.

6. Ako je to prihvatljivo pružaocu usluga, Strana može dostaviti nalog iz stava 1 i dopunske informacije iz stava 4 u elektronskom obliku. Strana može dostaviti obavještenje i dodatne informacije iz stava 5 u elektronskom obliku. Mogu se zahtijevati odgovarajući nivoi sigurnosti i autentifikacije.

7. Ako pružalac usluga obavijesti organ iz stava 4 tačka c da neće otkriti tražene podatke o pretplatnicima ili ako ne otkrije podatke o pretplatnicima kao odgovor na nalog iz stava 1 u roku od trideset dana od prijema naloga ili u roku određenom u stavu 4 tačka d, zavisno od toga koji je rok od ta dva duži, nadležni organi Strane izdavaoca mogu nakon toga zatražiti izvršenje naloga samo na osnovu člana 8 ili drugih oblika uzajamne pomoći. Strane mogu zahtijevati da pružalac usluga navede razlog za odbijanje otkrivanja podataka o pretplatnicima koje se traži nalogom.

8. Strana može, u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, izjaviti da Strana izdavalac mora od pružaoca usluga tražiti otkrivanje podataka o pretplatnicima prije nego što ih zatraži u skladu sa članom 8, osim ako Strana izdavalac dostavi opravdano objašnjenje zašto to nije učinila.

9. U trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, Strana može:

a) zadržati pravo da ne primjenjuje ovaj član; ili

b) ako otkrivanje određenih vrsta pristupnih brojeva na osnovu ovog člana ne bi bilo u skladu sa osnovnim načelima njenog domaćeg pravnog sistema, zadržati pravo da ne primjenjuje ovaj član na takve brojeve.

Odjeljak 3

Postupci kojima se unapređuje međunarodna saradnja između organa u otkrivanju pohranjenih računarskih podataka

Izvršavanje naloga druge Strane za ubrzano podnošenje podataka o pretplatnicima i podataka o saobraćaju

Član 8

1. Svaka Strana donosi zakonodavne i druge mjere koje su potrebne da se njeni nadležni organi ovlaste za izdavanje naloga koji se kao dio zahtjeva dostavlja drugoj Strani kako bi se pružalac usluga na teritoriji zamoljene Strane natjerao da dostavi navedene i pohranjene

- a) podatke o pretplatnicima, i
- b) podatke o saobraćaju

koje posjeduje ili kontroliše taj pružalac usluga, a koji su potrebni za konkretne krivične istrage ili postupke Strane.

2. Svaka Strana donosi zakonodavne i druge mjere koje su potrebne za izvršavanje naloga iz stava 1 koji je dostavila Strana molilja.

3. U svom zahtjevu Strana molilja dostavlja nalog iz stava 1, prateće informacije i sva posebna procesna uputstva zamoljenoj Strani.

a) U nalogu se navode:

- i organ izdavalac i datum izdavanja naloga;
- ii izjava da je nalog izdat u skladu sa ovim protokolom;
- iii naziv i adresa pružaoca odnosno pružalaca usluga kojima treba uručiti nalog;
- iv krivično djelo odnosno djela koja su predmet krivične istrage ili postupka;
- v organ koji traži informacije ili podatke, ako nije riječ o organu izdavaocu; i
- vi detaljni opis konkretnih informacija ili podataka koji se traže.

b) U pratećim informacijama, koje su dostavljene kako bi se zamoljenoj Strani pomoglo u izvršenju naloga i koje se pružaocu usluga ne smiju otkriti bez saglasnosti Strane molilje, navode se:

- i domaći pravni osnov na osnovu koga je organ ovlašćen za izdavanje naloga;
- ii zakonske odredbe i propisane kazne za krivično djelo odnosno djela koja se istražuju ili za koja se krivično goni;
- iii razlog zbog koga Strana molilja smatra da pružalac usluga posjeduje ili kontroliše podatke;
- iv sažetak činjenica koje se odnose na istragu ili postupak;

- v relevantnost informacija ili podataka za istragu ili postupak;
- vi kontakt podaci jednog ili više organa koji mogu pružiti dodatne informacije;
- vii da li je već zatraženo čuvanje informacija ili podataka, uključujući datum čuvanja i svaki primjenjivi referentni broj; i
- viii da li su informacije ili podaci već zatraženi drugim sredstvima i, ako jesu, na koji način.

c) Strana molilja može zahtijevati da zamoljena Strana sprovede posebna procesna uputstva.

4. Strana može, u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, i u bilo kojem drugom trenutku, izjaviti da su za izvršenje naloga iz stava 1 potrebne dodatne prateće informacije.

5. Zamoljena Strana prihvata zahtjeve u elektronskom obliku. Prije nego što prihvati zahtjev, može zahtijevati odgovarajuće nivoe sigurnosti i autentifikacije.

6. a) Zamoljena Strana, od datuma prijema svih informacija navedenih u st. 3 i 4 preuzima razumne napore da bi pružaocu usluga uručila zahtjev u roku od najkasnije četrdeset pet dana i nalaže da se zahtijevane informacije ili podaci pošalju najkasnije:

- i u roku od dvadeset dana za informacije o pretplatnicima; i
- ii u roku od četrdeset pet dana za podatke o saobraćaju.

b) Zamoljena Strana dužna je da obezbijedi, bez nepotrebnog odlaganja, prenos dostavljenih informacija ili podataka Strani molilji.

7. Ako zamoljena Strana ne može da postupi u skladu sa uputstvima iz stava 3 tačka c na zahtijevani način, odmah obavještava Stranu molilju i, ako je primjenjivo, navodi sve uslove pod kojima bi mogla da postupi u skladu sa tim uputstvima, nakon čega Strana molilja odlučuje da li zahtjev ipak treba izvršiti.

8. Zamoljena Strana može odbiti da izvrši zahtjev na osnovu razloga utvrđenih u članu 25 stav 4 ili članu 27 stav 4 Konvencije ili može odrediti uslove koje smatra potrebnim da dozvoli izvršenje zahtjeva. Zamoljena Strana može odložiti izvršenje zahtjeva iz razloga utvrđenih u članu 27 stav 5 Konvencije. Zamoljena Strana što je prije moguće obavještava Stranu molilju o odbijanju, uslovima ili odlaganju. Zamoljena Strana obavještava Stranu molilju i o drugim okolnostima koje će vjerovatno znatno odložiti izvršenje zahtjeva. Na ovaj član primjenjuje se član 28 stav 2 tačka b Konvencije.

9. a) Ako Strana molilja ne može da ispuni uslov koji je odredila zamoljena Strana u skladu sa stavom 8, odmah obavještava zamoljenu Stranu. Zamoljena Strana nakon toga odlučuje da li ipak treba dostaviti informacije ili materijale.

b) Ako Strana molilja prihvati uslov, obavezana je tim uslovom. Zamoljena Strana koja dostavlja informacije ili materijale pod takvim uslovom može od Strane molilje zahtijevati da u vezi sa tim uslovom objasni upotrebu takvih informacija ili materijala.

10. Svaka Strana, u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, generalnom sekretaru Savjeta Evrope saopštava i redovno ažurira kontakt podatke organa određenih za:

- a) podnošenje naloga u skladu sa ovim članom; i
- b) primanje naloga u skladu sa ovim članom.

11. Strana može, u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, izjaviti da zahtijeva da joj zahtjeve drugih Strana u skladu sa ovim članom podnosi centralni organ Strane molilje ili drugi organ koji su uzajamno odredile predmetne Strane.

12. Generalni sekretar Savjeta Evrope uspostavlja i redovno ažurira registar organa koje su Strane odredile u skladu sa stavom 10. Svaka Strana dužna je da obezbijedi da su podaci koje je dostavila za registar u svakom trenutku tačni.

13. U trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, Strana može zadržati pravo da ne primjenjuje ovaj član na podatke o saobraćaju.

Ubrzano otkrivanje pohranjenih računarskih podataka u hitnoj situaciji

Član 9

1. a) Svaka Strana donosi zakonodavne i druge mjere koje su potrebne, u hitnoj situaciji, da njena kontakt tačka za mrežu dostupnu 24 sata dnevno sedam dana u nedjelji iz člana 35 Konvencije (u daljem tekstu: kontakt tačka) pošalje zahtjev kontakt tački i primi zahtjev od kontakt tačke u drugoj Strani kojim se traži momentalna pomoć da se od pružaoca usluga na teritoriji te Strane obezbijedi ubrzano otkrivanje navedenih pohranjenih računarskih podataka koje posjeduje ili kontroliše taj pružalac usluga, bez zahtjeva za uzajamnu pomoć.

b) Strana može, u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, izjaviti da neće izvršavati zahtjeve iz stava 1 tačka a kojima se traži samo otkrivanje informacija o pretplatnicima.

2. Svaka Strana donosi zakonodavne i druge mjere koje su potrebne da se, u skladu sa članom 1, omogući:

a) njenim organima da traže podatke od pružaoca usluga na njenoj teritoriji nakon zahtjeva iz stava 1;

b) pružaocu usluga na njenoj teritoriji da otkrije zahtijevane podatke njenim organima kao odgovor na zahtjev iz stava 2 tačka a; i

c) njenim organima da pruže zahtijevane podatke Strani molilji.

3. U zahtjevu iz stava 1 navode se:

a) nadležni organ koji traži podatke i datum izdavanja zahtjeva;

b) izjava da je zahtjev izdat u skladu sa ovim protokolom;

c) naziv i adresa pružaoca odnosno pružalaca usluga koji posjeduju ili kontrolišu tražene podatke;

d) krivično djelo odnosno djela koja su predmet krivične istrage ili postupka i upućivanje na odgovarajuće zakonske odredbe i propisane kazne;

e) dovoljne činjenice koje dokazuju da postoji hitna situacija i objašnjenje kako su traženi podaci sa njom povezani;

f) detaljni opis traženih podataka;

g) sva posebna procesna uputstva; i

h) sve druge informacije koje mogu pomoći u pribavljanju otkrivanja zahtijevanih podataka.

4. Zamoljena Strana prihvata zahtjev u elektronskom obliku. Strana može prihvatiti i zahtjev poslat usmenim putem i može zahtijevati potvrdu u elektronskom obliku. Prije nego što prihvati zahtjev, može zahtijevati odgovarajuće nivoe sigurnosti i autentifikacije.

5. Strana može, u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, izjaviti da zahtjeva da Strane molilje, nakon izvršenja zahtjeva, zahtjev i sve dopunske informacije koje su poslate u prilog tog zahtjeva predaju u formatu i putem kanala, koji može uključivati i uzajamnu pomoć, koje odredi zamoljena Strana.

6. Zamoljena Strana po ubrzanom postupku obavještava Stranu molilju o svojoj odluci o zahtjevu iz stava 1 i, ako je primjenjivo, navodi sve uslove pod kojima bi pružila podatke i sve druge oblike saradnje koji bi bili dostupni.

7. a) Ako Strana molilja ne može da ispuni uslov koji je odredila zamoljena Strana u skladu sa stavom 6, odmah obavještava zamoljenu Stranu. Zamoljena Strana nakon toga odlučuje da li ipak treba dostaviti informacije ili materijale. Ako Strana molilja prihvati uslov, obavezana je tim uslovom.

b) Zamoljena Strana koja dostavlja informacije ili materijale pod takvim uslovom može od Strane molilje zahtijevati da u vezi sa tim uslovom objasni upotrebu takvih informacija ili materijala.

Odjeljak 4

Postupci koji se odnose na uzajamnu pomoć u hitnim situacijama

Uzajamna pomoć u hitnim situacijama

Član 10

1. Svaka Strana može po ubrzanom postupku zatražiti uzajamnu pomoć ako smatra da postoji hitna situacija. Zahtjev u skladu sa ovim članom uključuje, uz ostali propisani sadržaj,

opis činjenica koje dokazuju da postoji hitna situacija i na koji način se tražena pomoć odnosi na tu situaciju.

2. Zamoljena Strana prihvata takav zahtjev u elektronskom obliku. Prije nego što prihvati zahtjev, može zahtijevati odgovarajuće nivoe sigurnosti i autentifikacije.

3. Zamoljena Strana može po ubrzanom postupku zatražiti dopunske informacije kako bi ocijenila zahtjev. Strana molilja po ubrzanom postupku pruža takve dopunske informacije.

4. Nakon što se uvjeri da postoji hitna situacija i da su ispunjeni ostali uslovi za uzajamnu pomoć, zamoljena Strana po ubrzanom postupku odgovara na zahtjev.

5. Svaka Strana dužna je da obezbijedi da jedno lice iz njenog centralnog organa ili drugih organa odgovornih za odgovaranje na zahtjeve za uzajamnu pomoć bude dostupno dvadeset četiri sata, sedam dana u nedjelji, za potrebe odgovaranja na zahtjev u skladu sa ovim članom.

6. Centralni organ ili drugi organi odgovorni za uzajamnu pomoć Strane molilje i zamoljene Strane mogu uzajamno odrediti da se rezultati izvršenja zahtjeva u skladu sa ovim članom, ili njihov rani primjerak, mogu dostaviti Strani molilji putem kanala koji nije upotrijebljen za podnošenje zahtjeva.

7. Ako ne postoji ugovor ili dogovor o uzajamnoj pomoći na osnovu jednoobraznog ili recipročnog zakonodavstva koje je na snazi između Strane molilje i zamoljene Strane, na ovaj član primjenjuje se član 27 stav 2 tačka b i st. 3 do 8 i član 28 st. 2 do 4 Konvencije.

8. Ako takav ugovor ili dogovor postoji, ovaj član dopunjava se odredbama takvog ugovora ili dogovora, osim ako predmetne Strane zajednički odluče da umjesto toga primijene bilo koju ili sve odredbe Konvencije iz stava 7 ovog člana.

9. Svaka Strana može, u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, izjaviti da se zahtjevi mogu poslati i direktno njenim pravosudnim organima ili kanalima Međunarodne organizacije kriminalističke policije (INTERPOL) ili njenoj kontakt tački dostupnoj 24 sata dnevno sedam dana u nedjelji, uspostavljenoj u skladu sa članom 35 Konvencije. U takvim slučajevima jedan primjerak šalje se istovremeno i centralnom organu zamoljene Strane preko centralnog organa Strane molilje. Ako je zahtjev poslat direktno pravosudnom organu zamoljene Strane, a taj organ nije nadležan za postupanje po zahtjevu, zahtjev upućuje nadležnom domaćem organu i o tome direktno obavještava Stranu molilju.

Odjeljak 5

Postupci koji se odnose na međunarodnu saradnju ako nema važećih međunarodnih sporazuma

Videokonferencije

Član 11

1. Strana molilja može zatražiti, a zamoljena Strana može dozvoliti uzimanje iskaza i izjave svjedoka ili vještaka putem videokonferencije. Strana molilja i zamoljena Strana se konsultuju kako bi se olakšalo rješavanje svih pitanja koja se mogu pojaviti u vezi sa izvršenjem zahtjeva, uključujući, prema potrebi: koja Strana predsjedava; organi i lica koji treba da budu prisutni; da li će jedna ili obje Strane tražiti od svjedoka ili vještaka da položi zakletvu, dati mu upozorenja ili uputstva; način ispitivanja svjedoka ili vještaka; način na koji se propisno obezbjeđuju prava svjedoka ili vještaka; postupanje u slučaju pozivanja na privilegiju ili imunitet; postupanje sa prigovorima na pitanja ili odgovore; i da li jedna ili obje Strane pružaju usluge pisanog i usmenog prevođenja i prepisa.

2. a) Centralni organi zamoljene Strane i Strane molilje međusobno direktno komuniciraju za potrebe ovog člana. Zamoljena Strana može prihvatiti zahtjev u elektronskom obliku. Prije prihvatanja zahtjeva, može zahtijevati odgovarajuće nivoe sigurnosti i autentifikacije.

b) Zamoljena Strana obavještava Stranu molilju o razlozima za neizvršenje ili odlaganje izvršenja zahtjeva. Član 27 stav 8 Konvencije primjenjuje se na ovaj član. Ne dovodeći u pitanje nijedan drugi uslov koji zamoljena Strana može odrediti u skladu sa ovim članom, na ovaj član primjenjuje se član 28 st. 2 do 4 Konvencije.

3. Zamoljena Strana koja pruža pomoć u skladu sa ovim članom nastoji da obezbijedi prisustvo lica čiji se iskaz ili izjava traži. Prema potrebi, zamoljena Strana može, u mjeri u kojoj je to moguće u skladu sa njenim zakonodavstvom, preduzeti potrebne mjere da se svjedok ili vještak natjera da se pojavi u zamoljenoj Strani u utvrđeno vrijeme na utvrđenom mjestu.

4. Postupa se u skladu sa postupcima koji se odnose na održavanje videokonferencije koje je odredila Strana molilja, osim ako nijesu u skladu sa domaćim pravom zamoljene Strane. U slučaju neusklađenosti ili ako Strana molilja nije odredila postupak, zamoljena Strana primjenjuje postupak u skladu sa svojim domaćim pravom, ako nijesu drukčije uzajamno odredile Strana molilja i zamoljena Strana.

5. Ne dovodeći u pitanje bilo koju nadležnost u skladu sa domaćim pravom Strane molilje, ako tokom videokonferencije svjedok ili vještak:

a) namjerno da lažnu izjavu nakon što je zamoljena Strana, u skladu sa domaćim pravom zamoljene Strane, obavezala to lice da istinito svjedoči;

b) odbije da svjedoči nakon što je zamoljena Strana, u skladu sa domaćim pravom zamoljene Strane, obavezala to lice da svjedoči; ili

c) učini drugu povredu dužnosti koja je zabranjena domaćim pravom zamoljene Strane tokom takvog postupka;

to lice može se kazniti u zamoljenoj Strani na isti način kao da je takva radnja učinjena u njenom domaćem postupku.

6. a) Ako Strana molilja i zamoljena Strana nijesu uzajamno odredile drukčije, zamoljena Strana snosi sve troškove povezane sa izvršenjem zahtjeva na osnovu ovog člana, osim:

- i naknada vještaka;
- ii troškova pisanog i usmenog prevođenja i prepisa; i
- iii vanrednih troškova.

b) Ako bi izvršenje zahtjeva prouzrokovalo vanredne troškove, Strana molilja i zamoljena Strana međusobno se konsultuju kako bi odredile uslove pod kojima se zahtjev može izvršiti.

7. Ako se Strana molilja i zamoljena Strana međusobno dogovore:

a) odredbe ovog člana mogu se primjenjivati za potrebe održavanja audiokonferencija;

b) tehnologija za videokonferencije može se upotrebljavati u svrhe, ili za saslušanja, koje nijesu opisane u stavu 1, između ostalog i za potrebe identifikacije lica ili predmeta.

8. Ako zamoljena Strana odluči da dozvoli saslušanje osumnjičenog ili optuženog lica, može zahtijevati posebne uslove i zaštitne mjere u pogledu uzimanja iskaza ili izjave od tog lica ili dostavljanja obavještenja tom licu ili primjene procesnih mjera na to lice.

Zajednički istražni timovi i zajedničke istrage

Član 12

1. Nadležni organi dviju ili više Strana mogu na osnovu uzajamnog sporazuma uspostaviti i voditi zajednički istražni tim na svojim teritorijama kako bi se olakšale krivične istrage ili postupci ako se smatra da je pojačana koordinacija od posebne koristi. Predmetne Strane određuju nadležne organe.

2. Postupci i uslovi kojima se uređuje rad zajedničkih istražnih timova, kao što su njihove posebne svrhe; sastav; funkcije; trajanje i svako produženje; lokacija; organizacija; uslovi prikupljanja, prenosa i upotrebe informacija ili dokaza; uslovi povjerljivosti; i uslovi za uključivanje organa učesnika jedne Strane u istražne aktivnosti koje se odvijaju na teritoriji druge Strane, biće u skladu sa sporazumom tih nadležnih organa.

3. Strana može, u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, izjaviti da njen centralni organ mora da bude potpisnik sporazuma o uspostavljanju tima ili se sa njim saglasiti na drugi način.

4. Ti nadležni organi i organi učesnici komuniciraju direktno, s tim da Strane mogu uzajamno odrediti druge odgovarajuće kanale komunikacije kad izuzetne okolnosti iziskuju veću centralnu koordinaciju.

5. Ako je potrebno preduzeti istražne mjere na teritoriji jedne od predmetnih Strana, organi učesnici iz te Strane mogu zatražiti od svojih organa da preduzmu te mjere, a da pri tom druge Strane ne moraju da podnesu zahtjev za uzajamnu pomoć. Te mjere sprovode

organi te Strane na njenoj teritoriji pod uslovima koji se primjenjuju na osnovu domaćeg prava u domaćoj istrazi.

6. Upotreba informacija ili dokaza koje organi učesnici jedne Strane dostavljaju organima učesnicima drugih predmetnih Strana može se odbiti ili ograničiti na način utvrđen sporazumom opisanim u st. 1 i 2. Ako tim sporazumom nijesu utvrđeni uslovi za odbijanje ili ograničavanje upotrebe, Strane mogu upotrijebiti dostavljene informacije ili dokaze:

a) za potrebe za koje je sporazum sklopljen;

b) za otkrivanje, istraživanje i gonjenje krivičnih djela koja nijesu krivična djela za koja je sporazum sklopljen, uz prethodnu saglasnost organa koji su dostavili informacije ili dokaze. Međutim, saglasnost nije potrebna ako je osnovnim pravnim načelima Strane koja upotrebljava informacije ili dokaze propisano otkrivanje informacija ili dokaza radi zaštite prava optuženog lica u krivičnom postupku. U tom slučaju, ti organi bez nepotrebnog odlaganja obavještavaju organe koji su dostavili informacije ili dokaze; ili

c) za sprečavanje hitne situacije. U tom slučaju organi učesnici koji su primili informacije ili dokaze obavještavaju bez nepotrebnog odlaganja organe učesnike koji su dostavili informacije ili dokaze, osim ako je uzajamno određeno drukčije.

7. Ako ne postoji sporazum opisan u st. 1 i 2, zajedničke istrage mogu se preduzeti pod uzajamno dogovorenim uslovima koji se utvrđuju za svaki pojedinačni slučaj posebno. Ovaj stav primjenjuje se nezavisno od toga da li postoji ugovor ili dogovor o uzajamnoj pomoći na osnovu jednoobraznog ili recipročnog zakonodavstva koje je na snazi između predmetnih Strana.

Poglavlje III

Uslovi i zaštitne mjere

Uslovi i zaštitne mjere

Član 13

U skladu sa članom 15 Konvencije svaka Strana obezbjeđuje da uspostavljanje, sprovođenje i primjena ovlašćenja i postupaka predviđenih ovim protokolom bude u skladu sa uslovima i zaštitnim mjerama predviđenim njenim domaćim pravom, čime će se obezbijediti odgovarajuća zaštita ljudskih prava i sloboda.

Zaštita ličnih podataka

Član 14

1. Područje primjene

a) Ako nije drukčije predviđeno u stavu 1 tačke b i c, svaka Strana obrađuje lične podatke koje primi na osnovu ovog protokola u skladu sa st. 2 do 15 ovog člana.

b) Ako su u trenutku prijema ličnih podataka na osnovu ovog protokola Strana prenosilac i Strana primalac uzajamno obavezane međunarodnim sporazumom o uspostavljanju sveobuhvatnog okvira između tih Strana za zaštitu ličnih podataka, koji se primjenjuje na prenos ličnih podataka u svrhu sprečavanja, otkrivanja, istrage krivičnih djela i gonjenja za krivična djela i kojim je predviđeno da je obrada ličnih podataka na osnovu tog sporazuma u skladu sa odredbama zakonodavstva predmetnih Strana o zaštiti podataka, uslovi takvog sporazuma primjenjuju se, za mjere koje su obuhvaćene područjem primjene takvog sporazuma, na lične podatke primljene na osnovu Protokola umjesto st. 2 do 15, osim ako su se predmetne Strane sporazumjele drukčije.

c) Ako Strana prenosilac i Strana primalac nijesu uzajamno obavezane sporazumom opisanim u stavu 1 tačka b, mogu uzajamno odrediti da se prenos ličnih podataka na osnovu ovog protokola može izvršiti na osnovu drugih sporazuma ili dogovora između predmetnih Strana umjesto st. 2 do 15.

d) Svaka Strana smatra da obrada ličnih podataka u skladu sa stavom 1 tač. a i b ispunjava odredbe njenog pravnog okvira o zaštiti ličnih podataka za međunarodne prenose ličnih podataka i da se na osnovu tog pravnog okvira neće zahtijevati dalje odobrenje za prenos. Strana može odbiti ili spriječiti prenos podataka drugoj Strani na osnovu ovog protokola samo zbog zaštite podataka u skladu sa uslovima iz stava 15 kad se primjenjuje stav 1 tačka a; ili u skladu sa uslovima sporazuma ili dogovora iz stava 1 tač. b ili c kad se primjenjuje jedna od tih tačaka.

e) Ništa u ovom članu ne sprečava Stranu da primijeni strože zaštitne mjere na obradu ličnih podataka od strane njenih organa koji su primljeni na osnovu ovog protokola.

2. Svrha i upotreba

a) Strana koja je primila lične podatke obrađuje ih u svrhe opisane u članu 2. Ne smije dalje obrađivati lične podatke u neodgovarajuću svrhu i ne smije dalje obrađivati podatke kad to nije dopušteno njenim domaćim pravnim okvirom. Ovim članom ne dovodi se u pitanje mogućnost Strane prenosioca da u određenom slučaju odredi dodatne uslove u skladu sa ovim protokolom, međutim, takvi uslovi ne uključuju opšte uslove zaštite podataka.

b) Strana koja prima podatke obezbjeđuje, u skladu sa svojim domaćim pravnim okvirom, da su traženi i obrađeni lični podaci relevantni i da nijesu pretjerani u odnosu na svrhe takve obrade.

3. Kvalitet i integritet

Svaka Strana preduzima razumne korake kako bi obezbijedila da se lični podaci čuvaju tačno i potpuno i da su ažurirani u mjeri u kojoj je to potrebno i prikladno za zakonitu obradu ličnih podataka, imajući u vidu svrhe u koje se obrađuju.

4. Osjetljivi podaci

Obrada od strane Strane ličnih podataka koji otkrivaju rasno ili etničko porijeklo, politička mišljenja ili vjerska ili druga uvjerenja ili članstvo u sindikatima; genetskih podataka;

biometrijskih podataka koji se smatraju osjetljivima imajući u vidu rizike koji su s njima povezani; ili ličnih podataka koji se odnose na zdravlje ili seksualni život, vrši se isključivo uz odgovarajuće zaštitne mjere kako bi se spriječio rizik od neopravdanog štetnog uticaja upotrebe takvih podataka, naročito od nezakonite diskriminacije.

5. Periodi čuvanja

Svaka Strana čuva lične podatke samo onoliko dugo koliko je to potrebno i primjereno imajući u vidu svrhe obrade podataka u skladu sa stavom 2. Kako bi ispunila tu obavezu, dužna je da svojim domaćim pravnim okvirom predvidi posebne periode čuvanja ili periodično preispitivanje potrebe za daljim čuvanjem podataka.

6. Automatizovane odluke

Odluke koje proizvode znatne negativne posljedice za relevantne interese pojedinca na koga se odnose lični podaci ne smiju se zasnivati isključivo na automatizovanoj obradi ličnih podataka, osim ako je to dopušteno na osnovu domaćeg prava i uz odgovarajuće zaštitne mjere koje uključuju mogućnost ljudske intervencije.

7. Bezbjednost podataka i bezbjednosni incident

a) Svaka Strana dužna je da obezbijedi da ima uspostavljene odgovarajuće tehnološke, fizičke i organizacione mjere za zaštitu ličnih podataka, naročito od gubitka ili slučajnog ili neovlašćenog pristupa, otkrivanja, izmjene ili uništenja (u daljem tekstu: bezbjednosni incident).

b) Nakon otkrivanja bezbjednosnog incidenta u kojem postoji znatan rizik od materijalne ili nematerijalne štete pojedincima ili drugoj Strani, Strana koja prima podatke odmah procjenjuje njegovu vjerovatnoću i opseg i odmah preduzima odgovarajuće mjere za ublažavanje takve štete. Takve mjere uključuju obavještanje organa koji vrši prenos ili, u smislu odjeljka 2 Poglavlja II, jednog ili više organa određenih u skladu sa stavom 7 tačka c. Međutim, obavještenje može uključivati odgovarajuća ograničenja u pogledu daljeg prenosa obavještenja; može se odložiti ili izostaviti ako bi takvo obavještenje moglo da ugrozi nacionalnu bezbjednost ili odložiti ako bi takvo obavještenje moglo da ugrozi mjere za zaštitu javne bezbjednosti. Takve mjere uključuju i obavještanje pojedinca o kome je riječ, osim ako je Strana preduzela odgovarajuće mjere kako više ne bi postojao znatan rizik. Obavještanje pojedinca može se odložiti ili izostaviti pod uslovima iz stava 12 tačka a podtačka i. Obaviještena Strana može zahtijevati konsultovanje i dodatne informacije o incidentu i odgovoru na taj incident.

c) Svaka Strana, u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, obavještava generalnog sekretara Savjeta Evrope o organu ili organima koje treba obavijestiti na osnovu stava 7 tačka b u smislu odjeljka 2 Poglavlja II: dostavljene informacije mogu se naknadno izmijeniti.

8. Vođenje evidencije

Svaka Strana vodi evidenciju ili raspolaže drugim odgovarajućim sredstvima da pokaže na koji način se u nekom konkretnom slučaju pristupa podacima pojedinca, kako se upotrebljavaju i otkrivaju.)

9. Dalje dijeljenje unutar Strane

a) Ako organ Strane dostavi lične podatke koje je prvobitno primio na osnovu ovog protokola drugom organu te Strane, taj drugi organ obrađuje ih u skladu sa ovim članom, uz poštovanje stava 9 tačka b.

b) Izuzetno od stava 9 tačka a, Strana koja je izrazila rezervu u skladu sa članom 17 može svojim konstitutivnim državama ili sličnim teritorijalnim jedinicama dostaviti lične podatke koje je primila pod uslovom da je Strana uspostavila mjere kako bi organi koji ih primaju nastavili djelotvorno da štite podatke obezbjeđujući nivo zaštite podataka uporediv sa onim koji se pruža ovim članom.

c) U slučaju naznaka o nepravilnom sprovođenju ovog stava Strana prenosilac može zatražiti konsultovanje i relevantne informacije o tim naznakama.

10. Dalji prenos drugoj zemlji ili međunarodnoj organizaciji

a) Strana koja prima podatke može prenijeti lične podatke drugoj zemlji ili međunarodnoj organizaciji samo uz prethodno odobrenje organa koji vrši prenos ili, u smislu odjeljka 2 Poglavlja II, jednog ili više organa određenih u skladu sa stavom 10 tačka b.

b) U trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, svaka Strana obavještava generalnog sekretara Savjeta Evrope o organu ili organima koji daju odobrenje u smislu odjeljka 2 Poglavlja II; dostavljene informacije mogu se naknadno izmijeniti.

11. Transparentnost i obavještavanje

a) Svaka Strana dužna je da, objavljivanjem opštih obavještenja ili ličnim obavještenjem pojedincu čiji su lični podaci prikupljeni, obavijesti o:

- i pravnom osnovu i svrsi odnosno svrhama obrade;
- ii svim periodima čuvanja ili preispitivanja u skladu sa stavom 5, kako je primjenjivo;
- iii primiocima ili kategorijama primalaca kojima se takvi podaci otkrivaju; i
- iv dostupnim mogućnostima pristupa, ispravke i pravne zaštite.

b) Strana može za svako propisano lično obavještenje primijeniti razumna ograničenja na osnovu svog domaćeg pravnog okvira u skladu sa uslovima utvrđenim u stavu 12 tačka a podtačka i.

c) Ako se domaćim pravnim okvirom Strane prenosioca propisuje davanje ličnog obavještenja pojedincu čiji su podaci dostavljeni drugoj Strani, Strana prenosilac preduzima mjere kako bi druga Strana u trenutku prenosa bila obaviještena o tom uslovu i odgovarajućim kontakt podacima. Lično obavještenje ne daje se ako je druga Strana zahtijevala da pružanje podataka ostane povjerljivo, u slučaju da se primjenjuju uslovi za ograničenja iz stava 12 tačka a podtačka i. Nakon što se ta ograničenja ne budu više primjenjivala i kad se lično obavještenje može dostaviti, druga Strana preduzima mjere kako bi se Strana prenosilac obavijestila. Ako još uvijek nije obaviještena, Strana prenosilac ima

pravo da uputi zahtjeve Strani primaocu koja će informisati Stranu prenosioca da li treba zadržati ograničenje.

12. Pristup i ispravka

a) Svaka Strana dužna je da obezbijedi da svaki pojedinac čiji su lični podaci primljeni na osnovu ovog protokola ima pravo da traži i dobije, u skladu sa postupcima utvrđenim njenim domaćim pravnim okvirom i bez nepotrebnog odlaganja:

i pisani ili elektronski primjerak dokumentacije koja se čuva o tom licu koja sadrži lične podatke pojedinca i dostupne informacije o pravnom osnovu i svrsi obrade, periodima čuvanja i primaocima ili kategorijama primalaca podataka (u daljem testu: pristup), kao i informacije o dostupnim mogućnostima pravne zaštite; pri čemu se na pristup u određenom slučaju mogu primjenjivati proporcionalna ograničenja dozvoljena njenim domaćim pravnim okvirom, koja su u trenutku donošenja odluke potrebna za zaštitu prava i sloboda drugih lica ili važnih ciljeva od opšteg javnog interesa i kojima se uzimaju u obzir legitimni interesi pojedinca o kome je riječ;

ii ispravku ako su lični podaci pojedinca netačni ili su nepravilno obrađeni; ispravka uključuje – ako je potrebno i opravdano uzimajući u obzir razloge za ispravku i konkretni kontekst obrade – ispravku, dopunu, brisanje ili anonimizaciju, ograničavanje obrade ili blokiranje.

b) Ako su pristup ili ispravka uskraćeni ili ograničeni, Strana bez nepotrebnog odlaganja pojedincu dostavlja pisani odgovor koji se može dati i u elektronskom obliku kojim se taj pojedinac obavještava o uskraćivanju ili ograničenju. Navode se razlozi za takvo uskraćivanje ili ograničenje i pružaju informacije o dostupnim mogućnostima pravne zaštite. Svi troškovi nastali prilikom dobijanja pristupa trebalo bi da budu ograničeni na ono što je razumno i nije pretjerano.

13. Pravna sredstva u sudskom i vansudskom postupku

Svaka Strana dužna je da ima djelotvorna pravna sredstva u sudskom i vansudskom postupku za pružanje pravne zaštite u slučaju kršenja ovog člana.

14. Nadzor

Svaka Strana dužna je da ima jedan ili više javnih organa, koji samostalno ili zajedno, vrše nezavisne i djelotvorne nadzorne funkcije i ovlašćenja u odnosu na mjere utvrđene ovim članom. Funkcije i ovlašćenja tih organa koji djeluju samostalno ili zajedno uključuju istražna ovlašćenja, ovlašćenje da postupaju po pritužbama i sposobnost preduzimanja korektivnih mjera.

15. Konsultovanje i suspenzija

Strana može suspendovati prenos ličnih podataka drugoj Strani ako ima čvrste dokaze da druga Strana sistemski ili materijalno krši uslove iz ovog člana ili da je materijalno kršenje neizbježno. Neće suspendovati prenose bez odgovarajućeg obavještenja i učiniće to tek nakon što su predmetne Strane učestvovala u odgovarajućem periodu konsultacija a da nije postignuto rješenje. Međutim, Strana može privremeno suspendovati prenose u slučaju sistemskog ili materijalnog kršenja koje predstavlja znatnu i neposrednu opasnost po život ili

bezbjednost ili znatnu štetu za ugled ili novčanu štetu fizičkog lica; u tom slučaju odmah nakon toga obavještava drugu Stranu i započinje konsultacije sa drugom Stranom. Ako konsultacije nijesu dovele do rješenja, druga Strana može recipročno da suspenduje prenos ako ima čvrste dokaze da je suspenzija od strane Strane koja suspenduje prenos bila u suprotnosti sa uslovima iz ovog stava. Strana koja suspenduje prenos ukida suspenziju čim se ispravi kršenje koje opravdava suspenziju; istovremeno se ukida svaka recipročna suspenzija. Sa svim ličnim podacima prenesenim prije suspenzije i dalje se postupa u skladu sa ovim protokolom.

Poglavlje IV

Završne odredbe

Dejstva ovog protokola

Član 15

1. a) Član 39 stav 2 Konvencije primjenjuje se na ovaj protokol.
b) Strane koje su članice Evropske unije mogu u svojim međusobnim odnosima primjenjivati pravo Evropske unije kojim se uređuju pitanja iz ovog protokola.
c) Stav 1 tačka b ne utiče na punu primjenu ovog protokola između Strana koje su članice Evropske unije i drugih Strana.
2. Član 39 stav 3 Konvencije primjenjuje se na ovaj protokol.

Potpisivanje i stupanje na snagu

Član 16

1. Ovaj protokol biće otvoren za potpisivanje Stranama Konvencije koje mogu izraziti svoju saglasnost da budu obavezane:
 - a) potpisivanjem bez rezerve u pogledu potvrđivanja, prihvatanja ili odobrenja; ili
 - b) potpisivanjem uz rezervu u pogledu potvrđivanja, prihvatanja ili odobrenja, nakon čega slijedi potvrđivanje, prihvatanje ili odobrenje.
2. Isprave o potvrđivanju, prihvatanju ili odobrenju deponuju se kod generalnog sekretara Savjeta Evrope.
3. Ovaj protokol će stupiti na snagu prvog dana mjeseca koji slijedi nakon isteka perioda od tri mjeseca poslije datuma kada su pet Strana Konvencije izrazile svoju saglasnost da budu obavezane ovim protokolom, u skladu sa odredbama st. 1 i 2 ovog člana.

4. Za svaku Stranu Konvencije koja naknadno iskaže svoju saglasnost da bude obavezana ovim protokolom, Protokol stupa na snagu prvog dana mjeseca po isteku perioda od tri mjeseca poslije datuma na koji je Strana izrazila svoju saglasnost da bude obavezana ovim protokolom, u skladu sa odredbama st. 1 i 2 ovog člana.

Federalna klauzula

Član 17

1. Federalna država može da zadrži pravo da preuzme obaveze po ovom protokolu koje su u skladu sa njenim osnovnim principima koji uređuju odnos između njene centralne vlade i konstitutivnih država ili drugih sličnih teritorijalnih jedinica, pod uslovom da:

- a) Protokol se primjenjuje na centralnu vladu federalne države;
- b) zadržavanje tog prava ne utiče na obaveze da se obezbijedi saradnja koju traže druge Strane u skladu sa odredbama Poglavlja II; i
- c) odredbe člana 13 primjenjuju se na konstitutivne države ili druge slične teritorijalne jedinice federalne države.

2. Druga Strana može spriječiti organe, pružaoce ili subjekte na svojoj teritoriji da sarađuju prilikom odgovora na zahtjev ili nalog koji je direktno podnijela konstitutivna država ili druga slična teritorijalna jedinica federalne države koja je izrazila rezervu u skladu sa stavom 1, osim ako ta federalna država obavijesti generalnog sekretara Savjeta Evrope da konstitutivna država ili druga slična teritorijalna jedinica primjenjuje obaveze iz ovog protokola koje se primjenjuju na tu federalnu državu. Generalni sekretar Savjeta Evrope uspostavlja i redovno ažurira registar takvih obavještenja.

3. Druga Strana ne smije spriječiti organe, pružaoce ili subjekte na svojoj teritoriji da sarađuju sa konstitutivnom državom ili drugom sličnom teritorijalnom jedinicom na osnovu rezerve iz stava 1 ako je nalog ili zahtjev podnesen preko centralne vlade ili ako je sporazum o zajedničkom istražnom timu u skladu sa članom 12 zaključen uz učešće centralne vlade. U takvim situacijama centralna vlada dužna je da obezbijedi ispunjavanje važećih obaveza iz Protokola, pri čemu se, u pogledu zaštite ličnih podataka dostavljenih konstitutivnim državama ili sličnim teritorijalnim jedinicama, primjenjuju samo uslovi iz člana 14 stav 9 ili, ako je primjenjivo, uslovi sporazuma ili dogovora iz člana 14 stav 1 tač. b ili c.

4. U pogledu odredbi ovog protokola, čija primjena potpada pod nadležnost konstitutivnih država ili drugih sličnih teritorijalnih jedinica koje ustavni sistem federacije ne obavezuje da preduzmu zakonodavne mjere, centralna vlada će obavijestiti nadležne organe tih država o navedenim odredbama prilažući svoje pozitivno mišljenje, podstičući ih da preduzmu potrebne mjere da bi te odredbe sproveli.

Teritorijalna primjena

Član 18

1. Ovaj protokol primjenjuje se na teritoriju ili teritorije navedene u izjavi Strane u skladu sa članom 38 st. 1 ili 2 Konvencije ako takva izjava nije povučena na osnovu člana 38 stav 3.
2. Svaka Strana može, prilikom potpisivanja ovog protokola ili deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, izjaviti da se ovaj protokol neće primjenjivati na jednu ili više teritorija navedenih u izjavi Strane po članu 38 st. 1 i/ili 2 Konvencije.
3. Izjava data u skladu sa stavom 2 ovog člana može, u odnosu na bilo koju teritoriju navedenu u takvoj izjavi, biti povučena putem obavještenja upućenog generalnom sekretaru Savjeta Evrope. To povlačenje će stupiti na snagu prvog dana mjeseca po isteku tri mjeseca od dana prijema tog obavještenja od strane generalnog sekretara.

Rezerve i izjave

Član 19

1. Pisanim obavještenjem adresiranim na generalnog sekretara Savjeta Evrope, svaka Strana Konvencije može, u vrijeme potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, izjaviti da koristi mogućnost stavljanja rezerve odnosno rezervi predviđenih članom 7, stav 9 tač. a i b, članom 8 stav 13 i članom 17 ovog Protokola. Ne može se izraziti nijedna druga rezerva.
2. Pisanim obavještenjem adresiranim na generalnog sekretara Savjeta Evrope, svaka Strana Konvencije može, u trenutku potpisivanja ovog protokola ili prilikom deponovanja svoje isprave o potvrđivanju, prihvatanju ili odobrenju, dati izjavu odnosno izjave iz člana 7 stav 2 tačka b i stav 8, člana 8 stav 11, člana 9 stav 1 tačka b i stav 5, člana 10 stav 9, člana 12 stav 3 i člana 18 stav 2 ovog protokola.
3. Pisanim obavještenjem adresiranim na generalnog sekretara Savjeta Evrope, svaka Strana Konvencije daje izjavu odnosno izjave, obavještenja ili saopštenja iz člana 7 stav 5 tač. a i e, člana 8 st. 4 i 10 tač. a i b; člana 14 stav 7 tačka c i stav 10 tačka b, i člana 17 stav 2 ovog protokola u skladu sa uslovima koji su utvrđeni u tom dokumentu.

Status i povlačenje rezervi

Član 20

1. Strana koja je izrazila rezervu u skladu sa članom 19 stav 1 povlači tu rezervu, u cjelini ili djelimično, čim joj okolnosti to budu dozvolile. To povlačenje će stupiti na snagu na dan prijema obavještenja adresiranog na generalnog sekretara Savjeta Evrope. Ukoliko se u tom obavještenju navede da će povlačenje rezerve stupiti na snagu na dan koji je naveden u tom obavještenju, a taj dan bude poslije datuma kada je to obavještenje primio generalni sekretar, to povlačenje stupiće na snagu tog kasnijeg datuma.
2. Generalni sekretar Savjeta Evrope može, s vremena na vrijeme, zatražiti od Strana koje su izrazile jednu ili više rezervi u skladu sa članom 19 stav 1 da izvijeste o izgledima za povlačenje tih rezervi.

Izmjene

Član 21

1. Svaka Strana ovog protokola može predložiti izmjene ovog protokola, koje će generalni sekretar Savjeta Evrope proslijediti državama članicama Savjeta Evrope, i Stranama i potpisnicama Konvencije, kao i svakoj državi koja je pozvana da pristupi Konvenciji.
2. Svaka izmjena koju Strana predloži biće dostavljena Evropskom komitetu za pitanja kriminala (CDPC), koji će svoje mišljenje o toj predloženoj izmjeni dostaviti Komitetu ministara.
3. Komitet ministara će razmotriti predloženu izmjenu i mišljenje koje je dostavio Evropski komitet za pitanja kriminala (CDPC), i nakon konsultacija sa Stranama Konvencije, može usvojiti izmjenu.
4. Tekst svake izmjene koju usvoji Komitet ministara u skladu sa stavom 3 biće prosljeđen Stranama ovog protokola radi prihvatanja.
5. Svaka izmjena usvojena u skladu sa stavom 3 stupiće na snagu tridesetog dana nakon što sve Strane ovog protokola budu obavijestile generalnog sekretara o svom prihvatanju te izmjene.

Rješavanje sporova

Član 22

Član 45 Konvencije primjenjuje se na ovaj protokol.

Konsultacije Strana i procjena sprovođenja

Član 23

1. Član 46 Konvencije primjenjuje se na ovaj protokol.
2. Strane periodično procjenjuju djelotvornu primjenu i sprovođenje odredaba ovog protokola. Shodno se primjenjuje član 2 Poslovnika Odbora za Konvenciju o računarskom kriminalu revidiran 16. oktobra 2020. godine. Strane će pet godina nakon stupanja na snagu ovog protokola prvi put preispitati i mogu konsenzusom izmijeniti postupke iz tog člana kako se primjenjuju na ovaj protokol.
3. Preispitivanje člana 14 počinje nakon što deset Strana Konvencije izrazi saglasnost da budu obavezane ovim protokolom.

Otkazivanje

Član 24

1. Svaka Strana može, u svakom trenutku, otkazati ovaj protokol putem obavještenja adresiranog na generalnog sekretara Savjeta Evrope.
2. Takav otkaz stupa na snagu prvog dana u mjesecu po isteku tri mjeseca od dana prijema obavještenja od strane generalnog sekretara.
3. Otkazivanje Konvencije od strane Strane ovog protokola predstavlja otkazivanje ovog protokola.
4. Sa informacijama ili dokazima prenijetim prije datuma stupanja na snagu otkazivanja postupaće se i dalje u skladu sa ovim protokolom.

Obavještenje

Član 25

Generalni sekretar Savjeta Evrope obavještava države članice Savjeta Evrope, Strane i potpisnice Konvencije, kao i svaku državu koja je pozvana da pristupi Konvenciji o:

- a) svakom potpisivanju;
- b) deponovanju svake isprave o potvrđivanju, prihvatanju ili odobrenju;
- c) svakom datumu stupanju na snagu ovog protokola u skladu sa članom 16 st. 3 i 4;
- d) svim izjavama ili rezervama izraženim u skladu sa članom 19 ili povlačenju rezervi izvršenim u skladu sa članom 20;
- e) svakom aktu, obavještenju ili saopštenju koji se odnosi na ovaj protokol.

U potvrdu toga, dolje potpisani, za to propisno ovlašćeni, potpisuju ovaj protokol.

Sačinjeno u Strazburu, 12. maja 2022. godine, na engleskom i francuskom jeziku, s tim da su oba teksta podjednako autentična, u jednom primjerku koji će biti deponovan u arhivi Savjeta Evrope. Generalni sekretar Savjeta Evrope će ovjerene kopije dostaviti svim državama članicama Savjeta Evrope, Stranama i Potpisnicama Konvencije, kao i svakoj državi pozvanoj da pristupi Konvenciji.

Član 3

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u „Službenom listu Crne Gore – Međunarodni ugovori“.