6 (2022) Nr. 1

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 2022 Nr. 66

A. TITEL

Tweede aanvullend protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, inzake nauwere samenwerking en verstrekking van elektronisch bewijsmateriaal; Straatsburg, 12 mei 2022

Voor een overzicht van de verdragsgegevens, zie verdragsnummers 013833, 009852 en 010573 in de Verdragenbank.

B. TEKST

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 co-operation 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 has 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.

Article 9

– Expedited disclosure of stored computer data in an emergency

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 non- physical 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.

Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques

Préambule

Les États membres du Conseil de l'Europe et les autres États Parties à la Convention sur la cybercriminalité (STE n° 185; ci-après « la Convention »), ouverte à la signature à Budapest le 23 novembre 2001, signataires du présent Protocole,

Gardant à l'esprit la portée et l'impact de la Convention dans le monde entier;

Rappelant que la Convention est déjà complétée par le Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n° 189), ouvert à la signature à Strasbourg le 28 janvier 2003 (ci-après le « Premier Protocole »), pour ce qui est des Parties audit Protocole;

Prenant en compte les traités existants du Conseil de l'Europe relatifs à la coopération en matière pénale ainsi que d'autres accords et arrangements relatifs à la coopération en matière pénale conclus entre les Parties à la Convention;

Compte tenu également de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) telle qu'amendée par son Protocole d'amendement (STCE n° 223), ouvert à la signature à Strasbourg le 10 octobre 2018, et auquel tout État peut être invité à adhérer;

Reconnaissant l'utilisation croissante des technologies de l'information et de la communication, y compris des services internet, et l'augmentation de la cybercriminalité, qui constitue une menace pour la démocratie et l'État de droit, et que de nombreux États considèrent également comme une menace pour les droits de l'homme;

Reconnaissant également le nombre croissant de victimes de la cybercriminalité et l'importance d'obtenir justice pour ces victimes;

Rappelant que les gouvernements ont le devoir de protéger la société et les personnes contre le crime commis non seulement dans le monde réel mais aussi dans le monde virtuel, notamment en diligentant des enquêtes et des poursuites criminelles effectives;

Conscients que les preuves recueillies sous forme électronique de toute infraction pénale sont de plus en plus stockées sur des systèmes informatiques situés dans des juridictions étrangères, multiples ou inconnues, et convaincus que des mesures supplémentaires sont nécessaires pour obtenir légalement ces preuves afin de permettre une réponse effective par la justice pénale et de défendre l'État de droit;

Reconnaissant la nécessité d'une coopération accrue et plus efficace entre les États et le secteur privé et que, dans ce contexte, une plus grande clarté ou sécurité juridique est nécessaire pour les fournisseurs de services et autres entités concernant les circonstances dans lesquelles ils peuvent répondre à des demandes directes de divulgation de données électroniques émanant des autorités de justice pénale d'autres Parties;

Entendant donc renforcer encore la coopération concernant la cybercriminalité et le recueil de preuves sous forme électronique d'une infraction pénale aux fins d'enquêtes ou de procédures pénales spécifiques grâce à des outils supplémentaires relevant d'une entraide plus efficiente et d'autres formes de coopération entre autorités compétentes; de la coopération en situation urgente; et de la coopération directe entre autorités compétentes et fournisseurs de services et autres entités qui possèdent ou contrôlent les informations pertinentes;

Convaincus que des conditions et garanties effectives en matière de protection des droits de l'homme et des libertés fondamentales sont bénéfiques pour une coopération transfrontalière efficace aux fins de la justice pénale, y compris entre les secteurs public et privé;

Reconnaissant que la collecte de preuves électroniques pour les enquêtes pénales concerne souvent des données à caractère personnel, et reconnaissant l'exigence, dans de nombreuses Parties, de protéger la vie privée et les données à caractère personnel afin de satisfaire à leurs obligations constitutionnelles et internationales; et

Conscients de la nécessité de garantir que les mesures de justice pénale effective concernant la cybercriminalité et le recueil de preuves sous forme électronique sont soumises à des conditions et des garanties pour la protection appropriée des droits de l'homme et des libertés fondamentales, y compris des droits découlant d'obligations que les États ont contractées conformément à des instruments internationaux applicables en matière de droits de l'homme consacrés dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales de 1950 du Conseil de l'Europe (STE n° 5), dans le Pacte international relatif aux droits civils et politiques des Nations Unies de 1966, dans la Charte africaine des droits de l'homme et des peuples de 1981, dans la Convention américaine relative aux droits de l'homme de 1969 et dans d'autres traités internationaux relatifs aux droits de l'homme;

Sont convenus de ce qui suit:

CHAPITRE I

– DISPOSITIONS COMMUNES

Article 1

– But

Le présent Protocole a pour but de compléter:
a) la Convention entre les Parties au présent Protocole; et
b) le Premier Protocole entre les Parties au présent Protocole qui sont aussi Parties au Premier Protocole.

Article 2

– Champ d'application

1. Sauf dispositions contraires prévues au présent Protocole, les mesures qu'il énonce s'appliquent:
a) pour ce qui concerne les Parties à la Convention qui sont Parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des données et systèmes informatiques, ainsi qu'au recueil de preuves d'une infraction pénale sous forme électronique; et

b) pour ce qui concerne les Parties au Premier Protocole qui sont Parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques concernant les infractions pénales établies dans le Premier Protocole.

2. Chaque Partie adopte les mesures législatives ou autres pouvant se révéler nécessaires pour s'acquitter des obligations entérinées dans le présent Protocole.

Article 3

– Définitions

1. Les définitions indiquées aux articles 1 et 18, paragraphe 3, de la Convention s'appliquent au présent Protocole.

2. Aux fins du présent Protocole, les définitions supplémentaires ci-dessous s'appliquent:
a) l'expression « autorité centrale » s'entend de l'autorité ou des autorités désignées en vertu d'un traité ou d'un arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées, ou, à défaut, de l'autorité ou des autorités désignées par une Partie aux termes de l'article 27, paragraphe 2. a., de la Convention;
b) l'expression « autorité compétente » signifie une autorité judiciaire, administrative ou autre autorité chargée de l'application de la loi habilitée par le droit interne à ordonner, autoriser ou entreprendre l'exécution de mesures visées par le présent Protocole aux fins du recueil ou de la production de preuves concernant des enquêtes ou procédures pénales spécifiques;
c) le terme « urgence » signifie une situation présentant un risque grave et imminent pour la vie ou la sécurité d'une personne physique;
d) par « données à caractère personnel » on entend les informations relatives à une personne physique identifiée ou identifiable;
e) l'expression « Partie transférante » désigne la Partie qui transmet les données en réponse à une demande ou dans le cadre d'une équipe d'enquête commune, ou, aux fins de la section 2 du chapitre II, une Partie sur le territoire de laquelle se trouve un prestataire de services en mesure de transmettre ou une entité fournissant des services d'enregistrement de noms de domaine.

Article 4

– Langue

1. Les demandes, les injonctions et les renseignements qui les accompagnent présentés à une Partie doivent être rédigés dans une langue acceptable pour la Partie requise ou la Partie à laquelle ils sont notifiés en vertu de l'article 7, paragraphe 5, ou être accompagnés d'une traduction dans cette langue.

2. Les injonctions visées à l'article 7 et les demandes visées à l'article 6 et toute information qui les accompagne seront:
a) rédigées dans une langue de l'autre Partie dans laquelle le fournisseur de services ou l'entité les accepte en vertu d'une procédure nationale comparable;
b) rédigées dans une autre langue acceptable pour le fournisseur de services ou l'entité; ou
c) accompagnées d'une traduction dans l'une des langues visées aux paragraphes 2.a ou 2.b.

CHAPITRE II

– MESURES DE COOPERATION RENFORCEE

SECTION 1

– PRINCIPES GENERAUX APPLICABLES AU CHAPITRE II

Article 5

– Principes généraux applicables au chapitre II

1. Conformément aux dispositions du présent chapitre, les Parties s'assurent la coopération mutuelle la plus large possible.

2. La section 2 de ce chapitre se compose des articles 6 et 7. Elle prévoit des procédures renforçant la coopération directe avec les fournisseurs et les entités sur le territoire d'une autre Partie. La section 2 s'applique, qu'il existe ou non un traité ou un arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées.

3. La section 3 du présent chapitre est constituée des articles 8 et 9. Elle prévoit des procédures visant à renforcer la coopération internationale entre les autorités pour la divulgation de données informatiques stockées. La section 3 s'applique, qu'il existe ou non un traité ou un arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise.

4. La section 4 du présent chapitre est constituée de l'article 10. Elle prévoit des procédures relatives à l'entraide d'urgence. La section 4 s'applique qu'il existe ou non un traité ou un arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise.

5. La section 5 du présent chapitre est constituée des articles 11 et 12. La section 5 s'applique en l'absence de traité ou d'arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise. Les dispositions de la section 5 ne s'appliquent pas lorsqu'un traité ou un arrangement de ce type existe, sauf dans les cas prévus à l'article 12, paragraphe 7. Toutefois, les Parties concernées peuvent convenir d'appliquer à la place les dispositions de la section 5 si le traité ou arrangement ne l'interdit pas.

6. Lorsque, conformément aux dispositions du présent Protocole, la Partie requise est autorisée à subordonner la coopération à l'existence d'une double incrimination, cette condition est considérée comme satisfaite si le comportement constituant l'infraction pour laquelle l'entraide est requise est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

7. Les dispositions du présent chapitre ne restreignent pas la coopération entre les Parties, ou entre les Parties et les fournisseurs de services ou d'autres entités, par le biais d'autres accords, arrangements, pratiques ou le droit interne applicables.

SECTION 2 – PROCEDURES RENFORÇANT LA COOPERATION DIRECTE AVEC LES FOURNISSEURS ET LES ENTITES DANS LES AUTRES PARTIES

Article 6

– Demande d'informations concernant l'enregistrement d'un nom de domaine

1. Chaque Partie adopte les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes aux fins d'enquêtes ou procédures pénales spécifiques, à émettre auprès d'une entité fournissant des services d'enregistrement de noms de domaine située sur le territoire d'une autre Partie une demande d'informations en la possession ou sous le contrôle de l'entité en vue d'identifier ou de contacter la personne ayant enregistré un nom de domaine.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à une entité située sur son territoire de divulguer de telles informations en réponse à une demande introduite en vertu du paragraphe 1, sous réserve des conditions raisonnables prévues par le droit interne.

3. La demande visée au paragraphe 1 contient:
a) la date d'émission de la requête, l'identité et les coordonnées de l'autorité émettrice compétente;
b) le nom de domaine pour lequel les informations sont demandées et une liste détaillée des informations demandées, y compris les éléments de données particuliers;
c) une mention déclarant que la demande est émise en vertu du présent Protocole et que l'information est nécessaire du fait de la pertinence qu'elle revêt pour une enquête ou procédure pénale spécifique; et qu'elle ne sera utilisée que dans le cadre de cette enquête ou procédure pénale spécifique; et
d) le délai et le moyen de divulgation de ces informations et toutes autres instructions procédurales spéciales.

4. Si l'entité le juge acceptable, une Partie peut présenter une demande au titre du paragraphe 1 sous forme électronique. Des niveaux appropriés de sécurité et d'authentification peuvent être exigés.

5. Si une entité visée au paragraphe 1 ne coopère pas, la Partie requérante peut lui demander de motiver la non-divulgation des informations demandées. La Partie requérante peut envisager une consultation avec la Partie sur le territoire de laquelle l'entité est située en vue de déterminer les mesures disponibles pour obtenir les informations.

6. Chaque Partie, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, ou à tout autre moment, communique au Secrétaire Général du Conseil de l'Europe l'autorité désignée aux fins de consultation en vertu du paragraphe 5.

7. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités désignées par les Parties en vertu du paragraphe 6. Chaque Partie veille à ce que les informations qu'elle a fournies pour le registre soient exactes à tout moment.

Article 7

– Divulgation de données relatives aux abonnés

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à adresser directement à un fournisseur de services sur le territoire d'une autre Partie une injonction de produire des données spécifiées et stockées relatives à des abonnés, en la possession ou sous le contrôle du fournisseur, lorsque ces informations sont nécessaires à des enquêtes ou des procédures pénales spécifiques menées par la Partie émettrice.

2. a) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour qu'un fournisseur de services sur son territoire communique des données relatives aux abonnés en réponse à une injonction adressée en application du paragraphe 1.
b) Au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, une Partie peut – en ce qui concerne les injonctions adressées aux fournisseurs de services sur son territoire – faire la déclaration suivante: « l'injonction adressée en application de l'article 7, paragraphe 1, doit être émise par un procureur ou une autre autorité judiciaire, sous la supervision de cette autorité ou sous une autre forme de supervision indépendante. »

3. L'injonction, adressée en application du paragraphe 1, doit comprendre:
a) l'autorité émettrice et la date d'émission;
b) une déclaration indiquant que l'injonction est émise en vertu du présent Protocole;
c) le nom et l'adresse du ou des fournisseurs de services visés;
d) la ou les infractions faisant l'objet de l'enquête ou de la procédure pénale;
e) l'autorité qui sollicite les données spécifiques relatives aux abonnés, s'il ne s'agit pas de l'autorité émettrice; et
f) les données spécifiques relatives aux abonnés qui sont demandées, au moyen d'une description détaillée.

4. L'injonction adressée en application du paragraphe 1 doit être accompagnée des informations complémentaires suivantes:
a) le fondement juridique interne qui habilite l'autorité à adresser une injonction;
b) la mention des dispositions juridiques et des sanctions applicables à l'infraction qui est à l'origine d'une enquête ou de poursuites;
c) les coordonnées de l'autorité à laquelle le fournisseur de services doit communiquer les données relatives aux abonnés, à laquelle il peut demander de plus amples informations ou adresser toute autre réponse;
d) le délai et le mode de communication des données relatives aux abonnés;
e) l'indication d'une éventuelle demande de conservation des données précédemment formulée, en précisant la date de conservation et tout numéro de référence applicable;
f) tout type d'instructions spéciales en matière de procédure; et
g) le cas échéant, une déclaration selon laquelle la notification simultanée a été faite conformément au paragraphe 5; et
h) toute autre information qui pourrait aider à obtenir la divulgation des données relatives aux abonnés.

5. a) Une Partie peut, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, ou à tout autre moment, notifier au Secrétaire Général du Conseil de l'Europe qu'elle exige, lorsqu'une injonction est adressée en application du paragraphe 1 à un fournisseur de services sur son territoire, dans chaque cas ou dans certaines circonstances déterminées, la communication simultanée de l'injonction, des informations complémentaires et d'un résumé des faits relatifs à l'enquête ou à la procédure.
b) Qu'une Partie exige ou non la communication d'informations prévue au paragraphe 5.a, elle peut, dans certaines circonstances déterminées, demander au fournisseur de services de consulter les autorités de la Partie avant de divulguer les données demandées.
c) Les autorités informées en application du paragraphe 5.a ou consultées en application du paragraphe 5.b peuvent, dans les plus brefs délais, enjoindre au fournisseur de services de ne pas divulguer les données demandées, si:
   i) cette divulgation risque de porter préjudice à des enquêtes ou procédures pénales menées sur le territoire de cette Partie; ou
   ii) les conditions ou les motifs de refus visés aux articles 25, paragraphe 4, et 27, paragraphe 4, de la Convention s'appliquent parce que les données relatives aux abonnés ont fait l'objet d'une demande d'entraide.
d) Les autorités informées en application du paragraphe 5.a ou consultées en application du paragraphe 5.b:

i) peuvent demander des informations complémentaires à l'autorité visée au paragraphe 4.c aux fins de l'application du paragraphe 5.c et ne les divulgueront pas au fournisseur de services sans le consentement de cette autorité; et
ii) doivent informer rapidement l'autorité visée au paragraphe 4.c si le fournisseur de services a reçu pour instruction de ne pas divulguer les données demandées et doivent motiver cette décision.

e) Une Partie doit désigner une autorité unique pour recevoir la communication prévue au paragraphe 5.a et exécuter les tâches décrites aux paragraphes 5.b, 5.c. et 5.d. La Partie communique au Secrétaire Général du Conseil de l'Europe, au moment où la notification au Secrétaire Général prévue au paragraphe 5.a est faite pour la première fois, les coordonnées de cette autorité.
f) Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités désignées par les Parties conformément au paragraphe 5.e et note si elles exigent la communication d'informations prévue au paragraphe 5.a et dans quelles circonstances. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

6. Si le fournisseur de services le juge acceptable, une Partie peut soumettre une injonction en vertu du paragraphe 1 et des informations supplémentaires en vertu du paragraphe 4 sous forme électronique. Une Partie peut fournir la notification et les informations supplémentaires en vertu du paragraphe 5 sous forme électronique. Des niveaux appropriés de sécurité et d'authentification peuvent être exigés.

7. Si un fournisseur de services informe l'autorité visée au paragraphe 4.c qu'il ne divulguera pas les données demandées relatives aux abonnés ou s'il ne divulgue pas les données relatives aux abonnés en réponse à une injonction adressée en application du paragraphe 1 dans les trente jours suivant sa réception ou dans le délai prévu au paragraphe 4.d, la plus longue période étant retenue, les autorités compétentes de la Partie émettrice peuvent ensuite demander l'exécution de leur injonction uniquement au moyen de l'article 8 ou d'autres formes d'entraide. Les Parties peuvent demander au fournisseur de services de motiver son refus de divulguer les données relatives aux abonnés qui font l'objet de l'injonction.

8. Une Partie peut, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'une Partie émettrice doit solliciter la divulgation de données relatives aux abonnés auprès du fournisseur de services avant de la demander en vertu de l'article 8, à moins que la Partie émettrice ne fournisse une explication raisonnable justifiant de ne pas l'avoir fait.

9. Au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, une Partie peut:
a) se réserver le droit de ne pas appliquer cet article; ou
b) si la divulgation de certains types de numéros d'accès en vertu de cet article était incompatible avec les principes fondamentaux de son ordre juridique interne, se réserver le droit de ne pas appliquer cet article à ces numéros.

SECTION 3 – PROCEDURES RENFORÇANT LA COOPERATION INTERNATIONALE ENTRE AUTORITES POUR LA DIVULGATION DE DONNEES INFORMATIQUES STOCKEES

Article 8

– Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à délivrer une injonction à présenter dans le cadre d'une demande à une autre Partie aux fins d'ordonner à un fournisseur de services sur le territoire de la Partie requise de communiquer
a) des informations relatives à un abonné, et
b) des données relatives au trafic
spécifiées et stockées, en la possession ou sous le contrôle dudit fournisseur de services, lorsque ces informations et données sont nécessaires pour des enquêtes ou procédures pénales spécifiques menées par la Partie.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour donner effet à une injonction visée au paragraphe 1 soumise par une Partie requérante.

3. Dans sa demande, la Partie requérante soumet l'injonction visée au paragraphe 1, les informations qui l'accompagnent et toute instruction procédurale spéciale à la Partie requise.
a) L'injonction spécifie:
i) l'autorité émettrice et la date d'émission de la requête;
ii) une déclaration selon laquelle l'injonction est soumise en vertu du présent Protocole;
iii) le nom et l'adresse du ou des fournisseurs de services à laquelle elle doit être notifiée;
iv) la ou les infractions visées par l'enquête ou les poursuites pénales;

v) l'autorité à l'origine de la demande d'informations ou de données, si elle est différente de l'autorité ayant délivré l'injonction; et
vi) de manière détaillée les informations ou les données spécifiques demandées.

b) Les informations fournies à l'appui de l'injonction pour aider la Partie requise à lui donner effet et qui ne doivent pas être divulguées au fournisseur de services sans le consentement de la Partie requérante incluent:
i) les fondements juridiques en droit interne qui donnent à l'autorité le pouvoir d'émettre l'injonction;
ii) les dispositions légales et les sanctions applicables pour la ou les infractions objet de l'enquête ou des poursuites;
iii) la raison pour laquelle la Partie requérante pense que le fournisseur de services est en possession des données ou les contrôle;
iv) une synthèse des faits liés à l'enquête ou aux poursuites;
v) la pertinence des informations ou données pour l'enquête ou les poursuites;
vi) les éléments permettant de contacter une ou des autorités pour de plus amples informations;
vii) si la conservation des informations ou des données a déjà été demandée, auquel cas le document précisera la date de la demande et la cote de référence; et
viii) si les informations ou les données ont déjà été demandées par d'autres moyens et si oui, de quelle manière.

c) La Partie requérante peut demander que la Partie requise suive des instructions procédurales spécifiques.

4. Une Partie peut déclarer au moment de la signature du Protocole ou lors du dépôt de son instrument de ratification, d'acceptation, ou d'approbation, et à tout autre moment, que des informations supplémentaires sont nécessaires pour donner effet à des injonctions soumises en vertu du paragraphe 1.

5. La Partie requise accepte les demandes sous forme électronique; toutefois, avant de les accepter, elle peut exiger des niveaux de sécurité et d'authentification appropriés.

6. a) À compter de la date de réception de toutes les informations visées aux paragraphes 3 et 4, la Partie requise s'emploie raisonnablement à notifier l'injonction au fournisseur de services dans les quarante-cinq jours au plus en lui ordonnant de produire les informations en retour dans les:
i) vingt jours pour des informations relatives à l'abonné; et
ii) quarante-cinq jours pour les données relatives au trafic.

b) La Partie requise procède sans tarder à la transmission à la Partie requérante des informations ou données produites.

7. Si la Partie requise n'est pas en mesure d'appliquer sous la forme requise les instructions visées au paragraphe 3.c, elle en informe sans délai la Partie requérante et, au besoin, spécifie les conditions qui lui permettraient d'appliquer les instructions, à la suite de quoi la Partie requérante détermine si la demande doit malgré tout être exécutée.

8. La Partie requise peut invoquer les motifs visés à l'article 25, paragraphe 4, ou à l'article 27, paragraphe 4, de la Convention pour refuser l'exécution d'une demande ou peut imposer les conditions qu'elle estime nécessaires pour permettre l'exécution de la demande. La Partie requise peut invoquer les raisons visées à l'article 27, paragraphe 5, de la Convention pour ajourner l'exécution d'une demande. La Partie requise notifie dès que possible le refus, les conditions ou l'ajournement à la Partie requérante. La Partie requise notifie également à la Partie requérante les autres circonstances pouvant retarder de manière significative l'exécution de la demande. L'article 28, paragraphe 2.b de la Convention s'applique au présent article.

9. a) Si la Partie requérante ne peut se conformer à une condition imposée par la Partie requise en vertu du paragraphe 8, elle en informe rapidement la Partie requise. La Partie requise détermine alors si les informations ou le matériel devraient néanmoins être fournis.
b) Si la Partie requérante accepte la condition, elle est liée par celle-ci. La Partie requise qui fournit des informations ou du matériel soumis à une telle condition peut exiger de la Partie requérante qu'elle explique, en relation avec cette condition, l'utilisation qui a été faite de ces informations ou de ce matériel.

10. Au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation, ou d'approbation, chaque Partie communique au Secrétaire Général du Conseil de l'Europe et tient à jour les coordonnées des autorités désignées:
a) pour soumettre une injonction visée par le présent article; et
b) pour recevoir une injonction visée par le présent article.

11. Une Partie peut, au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'elle exige que les demandes des autres Parties visées par le présent article soient transmises par l'autorité ou les autorités centrales de la Partie requérante, ou par toute autre autorité désignée d'un commun accord entre les Parties concernées.

12. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités désignées par les Parties en vertu du paragraphe 10. Chaque Partie veille à ce que les coordonnées portées au registre soient en permanence correctes.

13. Au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, une Partie peut se réserver le droit de ne pas appliquer le présent article aux données relatives au trafic.

Article 9

– Divulgation accélérée de données informatiques stockées en situation d'urgence

1. a) Chaque Partie adopte les mesures législatives et autres pouvant se révéler nécessaires, en cas d'urgence, pour que son point de contact du Réseau 24/7 visé à l'article 35 de la Convention (« point de contact ») puisse transmettre une demande à un Point de contact dans une autre Partie et recevoir une demande de ce dernier pour une assistance immédiate en vue de l'obtention par un fournisseur de services situé sur le territoire de la Partie concernée de la divulgation accélérée de données informatiques stockées spécifiées qui sont en la possession ou sous le contrôle dudit fournisseur de services, sans requête d'entraide judiciaire.
b) Une Partie peut, au moment de la signature de ce Protocole ou au moment du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'elle n'exécutera pas de demandes introduites en vertu du paragraphe 1.a pour la divulgation d'informations relatives à l'abonné seulement.

2. Chaque Partie adopte les mesures législatives et autres pouvant se révéler nécessaires pour habiliter, conformément au paragraphe 1:
a) ses autorités à demander des données à un fournisseur de services situé sur son territoire à la suite d'une demande émise en vertu du paragraphe 1;
b) un fournisseur de services sur son territoire à divulguer les données demandées à ses autorités en réponse à une demande émise en vertu de l'alinéa 2.a; et
c) ses autorités à fournir les données demandées à la Partie requérante.

3. La demande introduite en vertu du paragraphe 1:
a) spécifie l'autorité compétente qui cherche des données et la date à laquelle la demande a été faite;
b) contient une déclaration selon laquelle la demande est émise en vertu du présent Protocole;
c) précise le nom et l'adresse du/des fournisseur(s) de services en possession des données recherchées ou qui en ont le contrôle;
d) précise la ou les infractions faisant l'objet de l'enquête ou des procédures pénales et indique la référence à ses dispositions légales et les sanctions applicables;
e) mentionne suffisamment de faits démontrant que la situation est urgente et comment les données demandées sont liées à la situation;
f) s'accompagne d'une description détaillée des données demandées;
g) précise les éventuelles instructions procédurales; et
h) mentionne toute autre information pouvant aider à obtenir la divulgation des données demandées.

4. La Partie requise accepte des demandes sous forme électronique. Une Partie peut également accepter des demandes transmises oralement et peut exiger une confirmation sous forme électronique. Elle peut exiger des niveaux appropriés de sécurité et d'authentification avant d'accepter la demande.

5. Une Partie peut, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'elle exige des Parties requérantes que celles-ci, après l'exécution de la demande, lui soumettent la demande et toutes informations supplémentaires transmises à l'appui de cette dernière, selon le format et le canal, qui peut couvrir une demande d'entraide judiciaire, spécifiés par la Partie requise.

6. La Partie requise informe la Partie requérante selon une procédure accélérée de sa détermination concernant la demande visée au paragraphe 1 et, au besoin, spécifie les éventuelles conditions dans lesquelles elle fournirait les données et toutes autres formes de coopération qui peuvent être utilisées.

7. a) Si une Partie requérante ne peut se conformer à une condition imposée par la Partie requise en vertu du paragraphe 6, elle en informe rapidement la Partie requise. La Partie requise détermine alors si les informations ou les documents devraient néanmoins être fournis. Si la Partie requérante accepte la condition, elle est liée par celle-ci.

b) La Partie requise qui fournit des renseignements ou du matériel soumis à une telle condition peut exiger de la Partie requérante qu'elle explique, en relation avec cette condition, l'utilisation qui a été faite de ces renseignements ou de ce matériel.

SECTION 4 – PROCEDURES RELATIVES A LA DEMANDE D'ENTRAIDE URGENTE

Article 10

– Demande d'entraide urgente

1. Chaque Partie peut demander une entraide judiciaire par les moyens les plus rapides lorsqu'elle estime qu'il y a urgence. Une demande d'entraide en vertu du présent article doit présenter, outre les autres contenus requis, une description des faits étayant l'existence d'une situation urgente et une explication de la manière dont l'entraide demandée est liée à cette situation.

2. La Partie requise accepte une telle demande d'entraide sous forme électronique. Elle peut exiger des niveaux de sécurité et d'authentification appropriés avant de l'accepter.

3. La Partie requise peut, par les moyens les plus rapides, demander un complément d'information afin d'évaluer la demande d'entraide. La Partie requérante fournit ce complément d'information par les moyens les plus rapides.

4. Après avoir conclu à l'existence d'une situation urgente et s'être assuré que les autres conditions de l'entraide sont satisfaites, la Partie requise répond à la demande d'entraide par les moyens les plus rapides.

5. Chaque Partie veille à ce qu'une personne de son autorité centrale ou d'autres autorités responsables des demandes d'entraide soit disponible vingt-quatre heures sur vingt-quatre, sept jours sur sept, pour répondre à une demande présentée en vertu du présent article.

6. L'autorité centrale ou les autres autorités responsables des demandes d'entraide des Parties requérante et requise peuvent décider de prévoir que les résultats de l'exécution d'une demande d'entraide effectuée en vertu du présent article, ou une copie préliminaire de ces résultats, peuvent être transmis à la Partie requérante par un canal autre que celui utilisé pour la transmission la demande.

7. Lorsqu'il n'existe pas de traité ou d'arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, l'article 27, paragraphes 2.b et 3 à 8, et l'article 28, paragraphes 2 à 4, de la Convention s'appliquent au présent article.

8. Lorsqu'un tel traité ou arrangement existe, le présent article est complété par les dispositions de ce traité ou arrangement, à moins que les Parties concernées ne décident d'un commun accord d'appliquer à la place l'une ou la totalité des dispositions de la Convention visées au paragraphe 7 du présent article.

9. Chaque Partie peut, au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer que des demandes d'entraide peuvent aussi être adressées directement par ses autorités judiciaires, ou par le biais de l'Organisation internationale de police criminelle (INTERPOL) ou du point de contact 24/7 établi au titre de l'article 35 de la Convention. Dans de tels cas, une copie est envoyée en même temps à l'autorité centrale de la Partie requise par le truchement de l'autorité centrale de la Partie requérante. Lorsqu'une demande est adressée directement à une autorité judiciaire de la Partie requise et que celle-ci n'est pas compétente pour traiter la demande, elle transmet la demande à l'autorité nationale compétente et en informe directement la Partie requérante.

SECTION 5 – PROCEDURES RELATIVES A LA COOPERATION INTERNATIONALE EN L'ABSENCE D'ACCORDS INTERNATIONAUX APPLICABLES

Article 11

– Vidéoconférence

1. Une Partie requérante peut demander, et la Partie requise peut autoriser, le recueil de la déposition d'un témoin ou d'un expert par vidéoconférence. La Partie requérante et la Partie requise se concertent pour faciliter la résolution de tous problèmes pouvant se poser concernant l'exécution de la demande, y compris le cas échéant le choix de la Partie qui dirige l'opération; les autorités et personnes qui seront présentes; si l'une des Parties ou les deux doivent demander au témoin ou à l'expert de prêter un serment particulier, lui dispenser des avertissements ou des instructions; la manière de questionner le témoin ou l'expert; la manière dont les droits du témoin ou de l'expert seront dûment garantis; le traitement des revendications de privilèges ou d'immunité; le traitement des objections aux questions ou réponses; et la question de savoir si l'une des Parties ou les deux assurent des services de traduction, d'interprétation et de transcription.

2. a) Les autorités centrales de la Partie requise et de la Partie requérante communiquent directement entre elles aux fins du présent article. Une Partie requise peut accepter une demande sous forme électronique. Elle peut exiger des niveaux appropriés de sécurité et d'authentification avant d'accepter la demande.
b) La Partie requise informe la Partie requérante des raisons pour lesquelles la demande n'a pas été exécutée ou a été retardée. L'article 27, paragraphe 8, de la Convention s'applique au présent article. Sans préjudice de toute autre condition qu'une Partie requise peut imposer conformément au présent article, les paragraphes 2 à 4 de l'article 28 de la Convention s'appliquent au présent article.

3. Une Partie requise fournissant son assistance au titre de cet article veille aux mesures nécessaires pour obtenir la présence de la personne dont le témoignage ou la déposition est requis. Le cas échéant, la Partie requise peut, dans la mesure où son droit le lui permet, prendre les mesures nécessaires pour obliger un témoin ou un expert à comparaître dans la Partie requise à l'endroit, à la date et à l'heure fixées.

4. Les procédures concernant la conduite de la vidéoconférence spécifiées par la Partie requérante sont appliquées, à moins qu'elles ne soient incompatibles avec le droit interne de la Partie requise. En cas d'incompatibilité, ou si la procédure n'a pas été spécifiée par la Partie requérante, la Partie requise applique la procédure prévue dans son droit interne sauf s'il en a été convenu autrement par les Parties requérante et requise.

5. Sans préjudice d'une éventuelle compétence en vertu du droit interne de la Partie requérante, lorsque, durant la vidéoconférence, le témoin ou l'expert:
a) fait intentionnellement une fausse déclaration alors que la Partie requise a, conformément à son droit interne, intimé à la personne auditionnée de dire la vérité dans sa déposition;
b) refuse de témoigner alors que la Partie requise a, conformément à son droit interne, astreint une telle personne à le faire; ou
c) commet tout autre acte interdit par le droit interne de la Partie requise au cours de l'audition;
il encourt dans la Partie requise la même sanction que si l'acte avait été commis dans le cadre des procédures prévues par le droit interne de cette dernière.

6. a) À moins que la Partie requérante et la Partie requise en aient décidé autrement, la Partie requise supporte tous les coûts liés à l'exécution d'une demande d'entraide en vertu de cet article, sauf:
   i) les honoraires d'un témoin expert;
   ii) les coûts de traduction, d'interprétation et de transcription; et
   iii) les dépenses exceptionnelles.
b) Si l'exécution d'une demande est susceptible d'entraîner des dépenses de nature exceptionnelle, la Partie requérante et la Partie requise se concertent pour déterminer dans quelles conditions la demande sera exécutée.

7. Lorsque la Partie requérante et la Partie requise en conviennent:
a) les dispositions du présent article peuvent être appliquées dans le but de réaliser des audioconférences;
b) la technologie de la vidéoconférence peut être utilisée à des fins, ou pour des auditions, différentes de celles visées au paragraphe 1, y compris en vue de l'identification de personnes ou d'objets.

8. Lorsqu'une Partie requise choisit d'autoriser l'audition d'un suspect ou d'un inculpé, elle peut poser des conditions et garanties particulières pour ce qui est du recueil du témoignage ou de la déposition de la personne, ou prévoir des notifications ou applications de mesures procédurales concernant cette personne.

Article 12

– Équipes communes d'enquête et enquêtes communes

1. Lorsqu'une coordination renforcée est considérée comme particulièrement utile, d'un commun accord, les autorités compétentes de deux ou plusieurs Parties peuvent établir et faire fonctionner une équipe commune d'enquête sur leurs territoires pour faciliter les enquêtes ou les poursuites. Les autorités compétentes sont déterminées par les Parties respectives concernées.

2. Les procédures et modalités régissant le fonctionnement d'équipes communes d'enquête, telles que leurs objectifs spécifiques; leur composition; leurs fonctions; leur durée et toute éventuelle prolongation; leur emplacement; leur organisation; le recueil, la transmission et l'utilisation des informations ou preuves; les conditions de confidentialité et les conditions de l'implication des autorités participantes d'une Partie dans des mesures d'enquête se déroulant sur le territoire d'une autre Partie, font l'objet d'un accord entre les autorités compétentes concernées.

3. Une Partie peut déclarer, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, que son autorité centrale doit être signataire de l'accord portant création de l'équipe ou y souscrire d'une autre manière.

4. Ces autorités compétentes et participantes communiquent directement entre elles, mais les Parties peuvent convenir d'un commun accord d'autres canaux de communication appropriés lorsque des circonstances exceptionnelles requièrent une coordination plus centrale.

5. Lorsque des mesures d'enquête doivent être prises sur le territoire de l'une des Parties concernées, les autorités participantes de cette Partie peuvent demander à leurs propres autorités de prendre ces mesures sans que les autres Parties aient à soumettre une demande d'entraide. Ces mesures doivent être mises en œuvre par les autorités de cette Partie sur son territoire aux mêmes conditions que celles s'appliquant en droit interne à une enquête nationale.

6. L'utilisation d'informations ou de preuves fournies par les autorités participantes d'une Partie aux autorités participantes d'autres Parties concernées peut être refusée ou limitée dans les conditions prévues à l'accord décrit aux paragraphes 1 et 2. Si un tel accord ne prévoit pas de conditions pour le refus ou la limitation de cette utilisation, les Parties peuvent utiliser les informations ou preuves fournies:

a) aux fins pour lesquelles l'accord a été conclu;
b) pour détecter, enquêter et poursuivre des infractions pénales autres que celles pour lesquelles l'accord a été conclu, sous réserve du consentement préalable des autorités qui ont fourni ces informations ou preuves. Le consentement ne sera toutefois pas requis lorsque les principes juridiques fondamentaux de la Partie utilisant les informations ou preuves exigent qu'elle divulgue ces dernières pour protéger les droits d'une personne poursuivie dans le cadre d'une procédure pénale. Dans ce cas, les autorités concernées doivent le notifier sans retard indu aux autorités qui ont fourni les informations ou preuves; ou
c) pour leur permettre de prévenir une urgence. Dans ce cas, les autorités participantes qui ont reçu les informations ou preuves doivent le notifier dans les plus brefs délais aux autorités participantes qui les ont fournies, sauf autre accord.

7. En l'absence d'accord tel que visé aux paragraphes 1 et 2, des enquêtes conjointes peuvent être mises en œuvre selon des modalités convenues au cas par cas. Ce paragraphe s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre les Parties concernées.

CHAPITRE III

– CONDITIONS ET GARANTIES

Article 13

– Conditions et garanties

Conformément à l'article 15 de la Convention, chaque Partie veille à ce que l'établissement, la mise en œuvre et l'application des pouvoirs et procédures prévus dans le présent Protocole soient soumis aux conditions et garanties prévues par son droit interne, qui doit assurer la protection adéquate des droits de l'homme et des libertés.

Article 14

– Protection des données à caractère personnel

1. Champ d'application

a) Sauf disposition contraire des paragraphes 1.b et c, chaque Partie traite les données à caractère personnel qu'elle reçoit au titre du présent Protocole conformément aux paragraphes 2 à 15 du présent article.
b) Si, au moment de la réception de données à caractère personnel en vertu du présent Protocole, la Partie transférante et la Partie destinataire sont toutes deux liées par un accord international établissant un cadre global entre ces Parties pour la protection des données à caractère personnel, applicable au transfert de données à caractère personnel aux fins de la prévention, de la détection, de l'investigation et de la poursuite d'infractions pénales, et qui prévoit que le traitement des données à caractère personnel en vertu de cet accord est conforme aux exigences de la législation sur la protection des données des Parties concernées, les termes de cet accord s'appliquent, pour les mesures relevant du champ d'application de cet accord, aux données à caractère personnel reçues en vertu de ce Protocole en lieu et place des paragraphes 2 à 15, sauf accord contraire entre les Parties concernées.
c) Si la Partie transférante et la Partie destinataire ne sont pas mutuellement liées par un accord décrit au paragraphe 1.b, elles peuvent déterminer d'un commun accord que le transfert de données à caractère personnel en vertu du présent Protocole peut avoir lieu sur la base d'autres accords ou arrangements entre les Parties concernées en lieu et place des paragraphes 2 à 15.
d) Chaque Partie considère que le traitement des données à caractère personnel conformément aux paragraphes 1.a et 1.b répond aux exigences de son cadre juridique de protection des données à caractère personnel pour les transferts internationaux de données à caractère personnel, et aucune autre autorisation de transfert n'est requise en vertu de ce cadre juridique. Une Partie ne peut refuser ou empêcher les

transferts de données vers une autre Partie en vertu du présent Protocole que pour des raisons de protection des données: dans les conditions énoncées au paragraphe 15, lorsque le paragraphe 1.a s'applique; ou aux termes d'un accord ou d'un arrangement visé aux paragraphes 1.b ou c, lorsque l'un de ces paragraphes s'applique.

e) Aucune disposition du présent article n'empêche une Partie d'appliquer des garanties plus strictes au traitement par ses propres autorités des données à caractère personnel reçues en vertu du présent Protocole.

2. But et utilisation

a) La Partie destinataire de données à caractère personnel traite lesdites données aux fins prévues à l'article 2. Elle ne procède pas à d'autres traitements des données à caractère personnel dans un but incompatible avec cet article, et elle ne traite pas non plus les données lorsque son cadre juridique ne l'autorise pas. Le présent article ne porte pas atteinte à la capacité de la Partie opérant le transfert d'imposer des conditions supplémentaires en vertu du présent Protocole dans une situation spécifique; toutefois, ces conditions n'incluent pas des conditions génériques de protection des données.

b) La Partie destinataire veille, dans le cadre de son droit interne, à ce que les données à caractère personnel demandées et traitées soient pertinentes et qu'elles ne soient pas excessives au regard de la finalité de ce traitement.

3. Qualité et intégrité

Chaque Partie prend des mesures raisonnables pour veiller à ce que les données à caractère personnel soient conservées de manière aussi exacte et complète et soient aussi actuelles qu'il est nécessaire et approprié pour qu'elles puissent être traitées conformément à la loi, compte tenu des buts dans lesquels elles sont traitées.

4. Données sensibles

Le traitement par une Partie de données à caractère personnel révélant l'origine ethnique ou raciale, les opinions politiques, les croyances religieuses ou autres, ou l'affiliation syndicale, ainsi que le traitement de données génétiques, de données biométriques considérées comme sensibles compte tenu des risques qu'elles comportent; ou de données à caractère personnel concernant la santé ou la sexualité; ne peut avoir lieu que moyennant des garanties appropriées pour se prémunir contre le risque d'effets préjudiciables injustifiés résultant de l'utilisation de ces données, en particulier contre la discrimination illicite.

5. Durées de conservation

Chaque Partie conserve les données à caractère personnel uniquement pour la durée nécessaire et appropriée, aux fins du traitement des données prévu au paragraphe 2. Pour s'acquitter de cette obligation, la Partie prévoit dans le cadre de son droit interne des durées de conservation spécifiques ou une révision périodique de l'opportunité de continuer à conserver les données.

6. Décisions automatisées

Les décisions ayant un effet défavorable significatif sur les intérêts pertinents de l'individu concerné par les données à caractère personnel ne peuvent pas être fondées uniquement sur un traitement automatisé des données à caractère personnel, sauf autorisation dans le droit interne et avec des garanties appropriées qui prévoient la possibilité d'obtenir une intervention humaine.

7. Sécurité des données et incidents de sécurité

a) Chaque Partie s'assure de disposer de mesures technologiques, physiques et organisationnelles appropriées pour la protection des données à caractère personnel, en particulier contre la perte ou l'accès, la divulgation, l'altération ou la destruction accidentels ou non autorisés (« incident lié à la sécurité »).

b) Dès qu'il est pris connaissance d'un incident de sécurité entraînant un risque significatif de préjudice matériel ou non matériel à des personnes ou à l'autre Partie, la Partie qui a reçu les données en évalue sans tarder la probabilité de survenance et l'importance, et prend rapidement les mesures appropriées pour atténuer ce préjudice. Ces mesures prennent la forme d'une notification à l'autorité transférante ou, aux fins du chapitre II, section 2, à l'autorité ou aux autorités désignées conformément au paragraphe 7.c. Cependant, la notification peut prévoir des restrictions appropriées concernant la transmission ultérieure de la notification; elle peut être différée ou omise lorsqu'elle risque de porter atteinte à la sécurité nationale, ou être retardée lorsque cette notification peut mettre en danger des opérations visant à protéger la sécurité publique. Ces mesures doivent également inclure une notification à la personne concernée, à moins que la Partie n'ait pris des mesures appropriées afin qu'il n'y ait plus de risque significatif. La notification à la personne concernée peut être différée ou omise dans les conditions énoncées au paragraphe 12.a.i. La Partie qui reçoit la notification peut demander une consultation et un complément d'information concernant l'incident et la réponse qui a été mise en œuvre.

c) Chaque Partie, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, indique au Secrétaire Général du Conseil de l'Europe quelles sont l'autorité ou les autorités qui reçoivent la notification visée au paragraphe 7.b, aux fins de la section 2 du chapitre II; celles-ci peuvent être modifiées ultérieurement.

8. Tenue des registres

Chaque Partie tient des registres ou se dote d'autres moyens appropriés pour montrer comment il est accédé aux données à caractère personnel d'un individu et comment celles-ci sont utilisées et divulguées dans un cas spécifique.

9. Partage ultérieur au sein d'une Partie

a) Lorsqu'une autorité d'une Partie fournit des données à caractère personnel reçues initialement en vertu du présent Protocole à une autre autorité de cette Partie, cette dernière les traite conformément au présent article, sous réserve du paragraphe 9.b.
b) Nonobstant le paragraphe 9.a, une Partie qui a fait une réserve en vertu de l'article 17 peut fournir des données à caractère personnel qu'elle a reçues à ses États constitutifs ou à des entités territoriales similaires, à condition que la Partie ait mis en place des mesures pour que les autorités qui reçoivent les données continuent à les protéger efficacement en assurant un niveau de protection des données comparable à celui offert par le présent article.
c) En cas d'indications d'une application incorrecte du présent paragraphe, la Partie transférante peut demander une consultation et des informations pertinentes sur ces indications.

10. Transfert ultérieur vers un autre État ou vers une organisation internationale

a) La Partie recevant les données à caractère personnel ne peut les transférer à un autre État ou à une organisation internationale qu'avec l'autorisation préalable de l'autorité qui les lui a communiquées ou, aux fins de la section 2 du chapitre II, de l'autorité ou des autorités désignées en vertu du paragraphe 10.b.
b) Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, l'autorité ou les autorités aux pouvoirs d'autorisation aux fins de la section 2 du chapitre II; ces informations peuvent être modifiées ultérieurement.

11. Transparence et notification

a) Chaque Partie assure les notifications par publication de notifications générales ou par notification spécifique à l'individu dont les données à caractère personnel ont été recueillies, concernant:
   i) la base juridique et le(s) but(s) du traitement;
   ii) toute durée de conservation ou de révision telle que visée au paragraphe 5, le cas échéant;
   iii) les destinataires ou les catégories de destinataires auxquels ces informations sont divulguées; et
   iv) l'accès, les rectifications ainsi que les recours possibles.
b) Une Partie peut soumettre toute exigence de notification personnelle à des restrictions raisonnables en vertu de son cadre juridique national conformément aux conditions énoncées au paragraphe 12.a.i.
c) Lorsque le droit interne de la Partie transférante exige que l'individu dont les données ont été fournies à une autre Partie soit informé personnellement, la Partie transférante prend des mesures pour que l'autre Partie soit informée au moment du transfert de cette exigence et des coordonnées appropriées. La notification personnelle n'est pas effectuée si l'autre Partie a demandé que la fourniture des données demeure confidentielle, dans la mesure où les conditions de restriction définies au paragraphe 12.a.i s'appliquent. Dès que ces restrictions ne s'appliquent plus et que la notification personnelle peut être effectuée, l'autre Partie prend des mesures pour que la Partie transférante soit informée. Si elle n'a pas encore été informée, la Partie transférante peut faire des demandes à la Partie destinataire qui informera la Partie transférante si la restriction doit être maintenue.

12. Accès et rectification

a) Chaque Partie veille à ce que toute personne dont les données à caractère personnel ont été reçues en application du présent Protocole ait le droit de demander et d'obtenir, conformément aux procédures établies dans son cadre juridique interne et sans retard excessif:
   i) l'accès à une copie écrite ou électronique de la documentation conservée sur cette personne, contenant ses données à caractère personnel et les informations disponibles indiquant la base juridique et les finalités du traitement, les périodes de conservation et les destinataires ou catégories de destinataires des données (« accès »), ainsi que les informations concernant les possibilités de recours disponibles à condition que l'accès dans un cas particulier puisse être soumis à l'application de restrictions proportionnées autorisées par son cadre juridique interne, nécessaires, au moment de la décision, pour protéger les droits et libertés d'autrui ou d'importants objectifs d'intérêt public général et qui tiennent dûment compte des intérêts légitimes de la personne concernée;
   ii) la rectification lorsque les données à caractère personnel de la personne sont inexactes ou ont été traitées de manière inappropriée; la rectification doit inclure, selon ce qui est approprié et raisonnable compte tenu des motifs de la demande de rectification et du contexte particulier du traitement, la correction, le complément, l'effacement ou l'anonymisation, la restriction du traitement ou le blocage.
b) Si l'accès ou la rectification est refusé ou restreint, la Partie en informe la personne concernée sous une forme écrite qui peut être envoyée par voie électronique, sans retard excessif, en informant l'individu du refus ou de la restriction. Elle indique les motifs de ce refus ou de cette restriction et fournit des informations sur les voies de recours disponibles. Les frais d'accès doivent être limités à ce qui est raisonnable et non excessif.

13. Recours judiciaire et non-judiciaire

Chaque Partie dispose d'un système permettant d'offrir des recours judiciaires et non judiciaires effectifs pour assurer la réparation des violations des garanties énoncées dans le présent article.

14. Supervision
Chaque Partie dispose d'une ou de plusieurs autorités publiques qui, ensemble ou séparément, exercent des fonctions et des compétences de supervision indépendantes et effectives à l'égard des mesures établies dans le présent article. Les fonctions et compétences exercées ensemble ou séparément par ces autorités comprennent des pouvoirs d'enquête, le pouvoir de donner suite aux plaintes, et la capacité de prendre des mesures correctives.

15. Consultation et suspension
Une Partie peut suspendre le transfert de données à caractère personnel à une autre Partie si elle dispose de preuves substantielles que celle-ci viole de manière systématique ou flagrante les dispositions du présent article ou qu'une violation flagrante est imminente. Cette suspension n'interviendra qu'à l'expiration d'un préavis raisonnable, et pas avant d'avoir engagé une période raisonnable de consultation sans parvenir à une résolution. Toutefois, une Partie peut suspendre provisoirement les transferts en cas de violation systématique ou flagrante présentant un risque important et imminent pour la vie ou la sécurité d'une personne physique, ou de préjudice financier ou de réputation pour cette personne, auquel cas cette Partie en informe l'autre et entame des consultations avec celle-ci immédiatement après. Si les délais de consultation ne permettent pas de trouver une solution, l'autre Partie peut suspendre les transferts si elle dispose de preuves substantielles que la suspension par la première Partie qui a procédé à la suspension était contraire aux termes du présent paragraphe. La Partie qui a procédé à la suspension la lève dès qu'il a été remédié à la violation justifiant la suspension; toute suspension réciproque est levée à ce moment. Toutes les données à caractère personnel transférées avant la suspension continuent à être traitées conformément au présent Protocole.

CHAPITRE IV

–CLAUSES FINALES

Article 15

– Effets de ce Protocole

1. a) L'article 39, paragraphe 2, de la Convention s'applique au présent Protocole.
b) En ce qui concerne les Parties qui sont membres de l'Union européenne: ces Parties peuvent, dans leurs relations mutuelles, appliquer les lois de l'Union européenne régissant les questions traitées dans le présent protocole.
c) Le paragraphe 1.b n'affecte pas la pleine application du présent Protocole entre les Parties qui sont membres de l'Union européenne et les autres Parties.

2. L'article 39, paragraphe 3, de la Convention s'applique au présent Protocole.

Article 16

– Signature et entrée en vigueur

1. Le présent Protocole est ouvert à la signature des Parties à la Convention, qui peuvent exprimer leur consentement à être liés par:
a) la signature sans réserve de ratification, d'acceptation ou d'approbation; ou
b) la signature sous réserve de ratification, d'acceptation ou d'approbation, suivie de ratification, d'acceptation ou d'approbation.

2. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

3. Le présent Protocole entre en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Parties à la Convention auront exprimé leur consentement à être liées par ce Protocole conformément aux dispositions des paragraphes 1 et 2 du présent article.

4. Pour toute Partie à la Convention qui exprime ultérieurement son consentement à être lié par ce Protocole, celui-ci entre en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle la Partie a exprimé son consentement à être liée par le Protocole, conformément aux dispositions des paragraphes 1 et 2 de cet article.

Article 17

– Clause fédérale

1. Un État fédéral peut se réserver le droit d'assumer les obligations découlant du présent Protocole conformément à ses principes fondamentaux régissant les relations entre son gouvernement central et les États constitutifs ou autres entités territoriales similaires, à condition que:
a) ce Protocole s'applique au gouvernement central de l'État fédéral;
b) une telle réserve n'affecte pas les obligations de fournir la coopération demandée par les autres Parties conformément aux dispositions du chapitre II; et
c) les dispositions de l'article 13 s'appliquent aux États constitutifs de l'État fédéral ou aux autres entités territoriales similaires.

2. Une autre Partie peut empêcher les autorités, les fournisseurs ou les entités sur son territoire de transférer des données à caractère personnel en réponse à une demande ou une injonction présentée directement par un État constitutif ou une autre entité territoriale similaire d'un État fédéral qui a formulé une réserve en vertu du paragraphe 1, à moins que l'État fédéral ne notifie au Secrétaire Général du Conseil de l'Europe qu'un État constitutif ou une autre entité territoriale similaire applique les obligations du présent Protocole applicables à cet État fédéral. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre de ces notifications.

3. Une autre Partie n'empêche pas les autorités, les fournisseurs ou les entités sur son territoire de coopérer avec un État constitutif ou une autre entité territoriale similaire en raison d'une réserve formulée en vertu du paragraphe 1, si un ordre ou une demande a été soumis par l'intermédiaire du gouvernement central ou si un accord relatif à une équipe commune d'enquête en vertu de l'article 12 est conclu avec la participation du gouvernement central. Dans ces situations, le gouvernement central assure l'exécution des obligations applicables de ce Protocole, étant entendu que, en ce qui concerne la protection des données à caractère personnel fournies aux États constitutifs ou aux entités territoriales similaires, seuls les termes de l'article 14, paragraphe 9, ou, le cas échéant, les termes d'un accord ou d'un arrangement décrit à l'article 14, paragraphes 1.b ou 1.c, s'appliquent.

4. En ce qui concerne les dispositions du présent Protocole dont l'application relève de la compétence des États constitutifs ou d'autres entités territoriales similaires, qui ne sont pas tenus par le système constitutionnel de la fédération de prendre des mesures législatives, le gouvernement central informe les autorités compétentes de ces États desdites dispositions avec son avis favorable, en les encourageant à prendre les mesures appropriées pour leur donner effet.

Article 18

– Application territoriale

1. Ce Protocole s'applique au(x) territoire(s) spécifiés dans une déclaration faite par une Partie en vertu de l'article 38, paragraphes 1 ou 2, de la Convention pour autant que cette déclaration n'ait pas été retirée en vertu de l'article 38, paragraphe 3.

2. Une Partie peut, au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer que ce Protocole ne s'applique pas à un ou plusieurs territoires spécifiés dans la déclaration de la Partie en vertu de l'article 38, paragraphes 1 et/ou 2, de la Convention.

3. Une déclaration en vertu du paragraphe 2 de cet article peut, concernant tout territoire qui y est spécifié, être retirée par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait devient effectif le premier jour du mois suivant l'expiration d'une période de trois mois après la date de la réception de cette notification par le Secrétaire Général.

Article 19

– Réserves et déclarations

1. Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie à la Convention peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, ou d'approbation, déclarer qu'elle se prévaut de la ou des réserves prévues à l'article 7, paragraphes 9.a et 9.b, à l'article 8, paragraphe 13 et à l'article 17 du présent Protocole. Aucune autre réserve ne peut être formulée.

2. Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie à la Convention peut, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation

ou d'approbation, faire la ou les déclarations prévues à l'article 7, paragraphes 2.b et 8, à l'article 8, paragraphe 11, à l'article 9, paragraphes 1.b et 5, à l'article 10, paragraphe 9, à l'article 12, paragraphe 3, et à l'article 18, paragraphe 2 du présent Protocole.

3. Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie à la Convention fait toute(s) déclaration(s), notifications ou communications visées à l'article 7, paragraphes 5.a et 5.e, à l'article 8, paragraphes 4, 10.a et 10.b, à l'article 14, paragraphes 7.c et 10.b, et à l'article 17, paragraphe 2, du présent Protocole selon les modalités qui y sont spécifiées.

Article 20

– Statut et retrait des réserves

1. Une Partie qui a fait une réserve conformément à l'article 19, paragraphe 1, retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent. Ce retrait prend effet à la date de réception d'une notification par le Secrétaire Général du Conseil de l'Europe. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2. Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves en application de l'article 19, paragraphe 1, des informations sur les perspectives de leur retrait.

Article 21

– Amendements

1. Toute Partie au Protocole peut proposer des amendements, qui sont communiqués par le Secrétaire Général du Conseil de l'Europe, aux États membres du Conseil de l'Europe et aux États Parties et signataires de la Convention ainsi qu'à tout État ayant été invité à adhérer à la Convention.

2. Tout amendement proposé par une Partie est communiqué au Comité européen sur les problèmes criminels (CDPC) qui soumet au Comité des Ministres son avis sur cet amendement proposé.

3. Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Parties à la Convention, peut adopter l'amendement.

4. Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 est transmis aux Parties à ce Protocole pour acceptation.

5. Tout amendement adopté conformément au paragraphe 3 entre en vigueur le trentième jour après que toutes les Parties à ce Protocole ont informé le Secrétaire Général qu'elles acceptent l'amendement.

Article 22

– Règlement des différends

L'article 45 de la Convention s'applique au présent Protocole.

Article 23

– Consultations des Parties et évaluation de la mise en œuvre

1. L'article 46 de la Convention s'applique au présent Protocole.

2. Les Parties évaluent périodiquement l'utilisation et la mise en œuvre effectives des dispositions du présent Protocole. L'article 2 du Règlement intérieur du Comité de la Convention sur la cybercriminalité tel que révisé le 16 octobre 2020 s'applique *mutatis mutandis*. Les Parties réexaminent initialement et peuvent modifier les procédures de cet article telles qu'elles s'appliquent au présent Protocole par consensus cinq ans après l'entrée en vigueur du présent Protocole.

3. L'examen de l'article 14 débute lorsque dix Parties à la Convention ont exprimé leur consentement à être liées par le présent Protocole.

Article 24

– Dénonciation

1. Toute Partie peut, à tout moment, dénoncer le présent Protocole par notification au Secrétaire Général du Conseil de l'Europe.

2. Ladite dénonciation prendra effet le premier jour du mois suivant l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

3. La dénonciation de la Convention par une Partie au présent Protocole constitue une dénonciation du présent Protocole.

4. Les informations ou éléments de preuve transférés avant la date de prise d'effet de la dénonciation continuent d'être traités conformément au présent Protocole.

Article 25

– Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux États membres du Conseil de l'Europe, aux Parties à la Convention et Signataires de la Convention, et à tout État qui a été invité à adhérer à la Convention:
a) toute signature;
b) le dépôt de tout instrument de ratification, d'acceptation ou d'approbation;
c) la date d'entrée en vigueur du présent Protocole conformément à l'article 16, paragraphes 3 et 4;
d) toutes déclarations ou réserves formulées conformément à l'article 19 ou retrait de réserves formulé conformément à l'article 20;
e) tout autre acte, notification ou communication concernant le présent Protocole.

EN FOI DE QUOI, les soussignés, dûment autorisés, ont apposé leur signature au bas du présent Protocole.

FAIT à Strasbourg, le 12 mai 2022, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui est déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe communiquera une copie certifiée conforme à chacun des États membres du Conseil de l'Europe, aux Parties et Signataires de la Convention, ainsi qu'à tout État invité à adhérer à la Convention.

C. VERTALING

Tweede aanvullend protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, inzake nauwere samenwerking en verstrekking van elektronisch bewijsmateriaal

Preambule

De lidstaten van de Raad van Europa en de andere staten die partij zijn bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (ETS nr. 185, hierna „het verdrag" genoemd), op 23 november 2001 te Boedapest opengesteld voor ondertekening, die dit protocol hebben ondertekend,

Indachtig het feit dat het verdrag betrekking heeft op en gevolgen heeft voor alle delen van de wereld;

Eraan herinnerend dat het verdrag reeds is aangevuld met het aanvullend protocol betreffende de strafbaarstelling van handelingen van racistische en xenofobische aard verricht via computersystemen (ETS nr. 189), voor ondertekening opengesteld op 28 januari 2003 te Straatsburg (hierna „het eerste protocol" genoemd), van toepassing tussen de partijen bij dat protocol;

Gezien de bestaande verdragen van de Raad van Europa inzake samenwerking op strafrechtelijk terrein, alsmede andere overeenkomsten en regelingen inzake samenwerking op strafrechtelijk terrein tussen de partijen bij het verdrag;

Gezien tevens het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108), gewijzigd bij het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (CETS nr. 223), voor ondertekening opengesteld op 10 oktober 2018 te Straatsburg, waartoe iedere staat kan worden uitgenodigd toe te treden;

Erkennende het toenemende gebruik van informatie- en communicatietechnologieën, met inbegrip van internetdiensten, en de toename van cybercriminaliteit, die een bedreiging vormt voor de democratie en de rechtsstaat en door veel staten ook als bedreiging voor de mensenrechten wordt beschouwd;

Erkennende tevens het groeiende aantal slachtoffers van cybercriminaliteit en het belang om recht te laten geschieden voor die slachtoffers;

Eraan herinnerend dat op overheden de verplichting rust om de samenleving en personen te beschermen tegen misdaad, niet alleen offline maar ook online, onder meer door op doeltreffende wijze strafrechtelijk onderzoek en strafrechtelijke vervolging in te stellen;

Beseffende dat bewijzen van strafbare feiten steeds vaker in elektronische vorm worden opgeslagen op computersystemen in verschillende buitenlandse of onbekende rechtsgebieden, en ervan overtuigd dat aanvullende maatregelen vereist zijn om dergelijke bewijzen rechtmatig te verkrijgen, teneinde strafrechtelijk doeltreffend op te treden en de rechtsstaat te handhaven;

Erkennende dat er behoefte is aan meer en efficiëntere samenwerking tussen staten en de particuliere sector, en dat in dit verband meer duidelijkheid en rechtszekerheid moet worden geboden aan serviceproviders en andere entiteiten met betrekking tot de omstandigheden waarin zij kunnen reageren op rechtstreekse verzoeken van strafrechtelijke autoriteiten in andere partijen om verstrekking van elektronische gegevens;

Strevende derhalve naar verdere versterking van de samenwerking op het gebied van cybercriminaliteit en de vergaring van bewijs in elektronische vorm van enig strafbaar feit met het oog op specifieke strafrechtelijke onderzoeken of procedures door middel van aanvullende instrumenten voor efficiëntere wederzijdse bijstand en andere vormen van samenwerking tussen bevoegde autoriteiten; van de samenwerking in noodsituaties; en van rechtstreekse samenwerking tussen bevoegde autoriteiten en serviceproviders en andere entiteiten die in het bezit zijn van relevante informatie of gerechtigd zijn tot toegang daartoe;

Ervan overtuigd dat doeltreffende grensoverschrijdende samenwerking voor strafrechtelijke doeleinden, ook tussen de openbare en de particuliere sector, baat heeft bij doeltreffende voorwaarden en waarborgen voor de bescherming van de mensenrechten en de fundamentele vrijheden;

Erkennende dat vergaring van elektronisch bewijsmateriaal voor strafrechtelijk onderzoek vaak betrekking heeft op persoonsgegevens, en erkennende dat veel partijen verplicht zijn privacy en persoonsgegevens te beschermen om hun grondwettelijke en internationale verplichtingen na te komen; en

Indachtig de noodzaak ervoor te zorgen dat doeltreffende strafrechtelijke maatregelen tegen cybercriminaliteit en de vergaring van bewijsmateriaal in elektronische vorm onderworpen zijn aan voorwaarden en waarborgen die voorzien in passende bescherming van de mensenrechten en de fundamentele vrijheden, met inbegrip van rechten die voortvloeien uit verplichtingen die staten zijn aangegaan in het kader van toepasselijke internationale mensenrechteninstrumenten, zoals het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden van 1950 (ETS nr. 5) van de Raad van Europa, het Internationaal Verdrag van de Verenigde Naties inzake burgerrechten en politieke rechten van 1966, het Afrikaans Handvest van de rechten van mensen en volken van 1981, het Amerikaans Verdrag inzake de rechten van de mens van 1969 en andere internationale mensenrechtenverdragen;

Zijn als volgt overeengekomen:

HOOFDSTUK I

– GEMEENSCHAPPELIJKE BEPALINGEN

Artikel 1

– Doel

Dit protocol strekt tot aanvulling van:
a. het verdrag zoals dat tussen de partijen bij dit protocol van toepassing is; en
b. het eerste protocol zoals dat van toepassing is tussen de partijen bij dit protocol die ook partij zijn bij het eerste protocol.

Artikel 2

– Toepassingsgebied

1. Tenzij anders bepaald, zijn de in dit protocol omschreven maatregelen van toepassing:
a. tussen partijen bij het verdrag die partij zijn bij dit protocol: op specifieke strafrechtelijke onderzoeken en procedures die betrekking hebben op strafbare feiten die verband houden met computersystemen en -gegevens, en op de vergaring van bewijs in elektronische vorm van enig strafbaar feit; en

b. tussen partijen bij het eerste protocol die partij zijn bij dit protocol: op specifieke strafrechtelijke onderzoeken en procedures die betrekking hebben op strafbare feiten zoals vastgesteld krachtens het eerste protocol.

2. Iedere partij neemt de wetgevende en andere maatregelen die nodig zijn om de in dit protocol genoemde verplichtingen na te komen.

Artikel 3

– Definities

1. De definities in artikel 1 en artikel 18, lid 3, van het verdrag zijn op dit protocol van toepassing.

2. Voor de toepassing van dit protocol wordt bovendien verstaan onder:
a. „centrale autoriteit": de autoriteit of autoriteiten die krachtens een verdrag of regeling inzake wederzijdse bijstand zijn aangewezen op basis van tussen de betrokken partijen geldende uniforme of wederkerige wetgeving, of, bij gebreke daarvan, de autoriteit of autoriteiten die een partij heeft aangewezen uit hoofde van artikel 27, lid 2, punt a), van het verdrag;
b. „bevoegde autoriteit": een gerechtelijke, bestuurlijke of andere rechtshandhavingsinstantie die krachtens het nationale recht bevoegd is om de uitvoering van maatregelen uit hoofde van dit protocol te gelasten, toe te staan of uit te voeren met het oog op het vergaren of verstrekken van bewijsmateriaal met betrekking tot specifieke strafrechtelijke onderzoeken of procedures;
c. „noodsituatie": een situatie waarin er een aanzienlijk en imminent risico bestaat voor het leven of de veiligheid van een natuurlijke persoon;
d. „persoonsgegevens": informatie over een geïdentificeerde of identificeerbare natuurlijke persoon;
e. „doorgevende partij": de partij die de gegevens doorzendt naar aanleiding van een verzoek of in het kader van een gemeenschappelijk onderzoeksteam of, voor de toepassing van hoofdstuk II, afdeling 2, een partij op het grondgebied waarvan zich een serviceprovider die doorgiftediensten aanbiedt of een entiteit die domeinnaamregistratiediensten aanbiedt, bevindt.

Artikel 4

– Taal

1. Verzoeken, bevelen en begeleidende informatie die bij een partij worden ingediend, worden gesteld in een taal die aanvaardbaar is voor de aangezochte partij of de partij waaraan overeenkomstig artikel 7, lid 5, kennisgeving wordt gedaan, of gaan vergezeld van een vertaling in een dergelijke taal.

2. De in artikel 7 bedoelde bevelen en de in artikel 6 bedoelde verzoeken en de begeleidende informatie daarbij:
a. worden ingediend in een taal van de andere partij waarin de serviceprovider of entiteit vergelijkbare binnenlandse bevelen of verzoeken aanvaardt;
b. worden ingediend in een andere taal die aanvaardbaar is voor de serviceprovider of entiteit; of
c. gaan vergezeld van een vertaling in een van de talen als bedoeld in lid 2, punt a) of b).

HOOFDSTUK II

– MAATREGELEN TER VERSTERKING VAN DE SAMENWERKING

AFDELING 1 – ALGEMENE BEGINSELEN VAN TOEPASSING OP HOOFDSTUK II

Artikel 5

– Algemene beginselen van toepassing op hoofdstuk II

1. De partijen werken zoveel mogelijk samen overeenkomstig de bepalingen van dit hoofdstuk.

2. Afdeling 2 van dit hoofdstuk bestaat uit de artikelen 6 en 7. Zij voorziet in procedures ter versterking van de rechtstreekse samenwerking met serviceproviders en entiteiten op het grondgebied van een andere partij. Afdeling 2 is van toepassing ongeacht of er sprake is van een verdrag of regeling inzake wederzijdse bijstand op basis van uniforme of wederkerige wetgeving tussen de betrokken partijen.

3. Afdeling 3 van dit hoofdstuk bestaat uit de artikelen 8 en 9. Zij voorziet in procedures ter versterking van de internationale samenwerking tussen autoriteiten bij de verstrekking van opgeslagen computergegevens. Afdeling 3 is van toepassing ongeacht of er sprake is van een verdrag of regeling inzake wederzijdse bijstand op basis van uniforme of wederkerige wetgeving tussen de verzoekende en de aangezochte partij.

4. Afdeling 4 van dit hoofdstuk bestaat uit artikel 10. Zij voorziet in procedures voor wederzijdse bijstand in noodsituaties. Afdeling 4 is van toepassing ongeacht of er sprake is van een verdrag of regeling inzake wederzijdse bijstand op basis van uniforme of wederkerige wetgeving tussen de verzoekende en de aangezochte partij.

5. Afdeling 5 van dit hoofdstuk bestaat uit de artikelen 11 en 12. Afdeling 5 is van toepassing wanneer er geen verdrag of regeling inzake wederzijdse bijstand op basis van uniforme of wederkerige wetgeving van kracht is tussen de verzoekende en de aangezochte partij. De bepalingen van afdeling 5 zijn niet van toepassing wanneer een dergelijk verdrag of een dergelijke regeling wel bestaat, behoudens het bepaalde in artikel 12, lid 7. De betrokken partijen kunnen evenwel onderling besluiten de bepalingen van afdeling 5 in plaats daarvan toe te passen, indien het verdrag of de regeling dat niet verbiedt.

6. Wanneer het de aangezochte partij, in overeenstemming met de bepalingen van dit protocol, is toegestaan medewerking afhankelijk te maken van het bestaan van dubbele strafbaarheid, wordt aan deze voorwaarde geacht te zijn voldaan indien de gedraging die ten grondslag ligt aan het strafbare feit waarvoor om medewerking wordt verzocht, in haar wetgeving wordt aangemerkt als strafbaar feit, ongeacht of het interne recht het strafbare feit al dan niet in dezelfde categorie plaatst of met dezelfde termen aanduidt als het recht van de verzoekende partij.

7. De bepalingen van dit hoofdstuk houden geen beperking in van de samenwerking tussen partijen, of tussen partijen en serviceproviders of andere entiteiten, op grond van andere toepasselijke overeenkomsten, regelingen, praktijken of het nationale recht.

AFDELING 2 – PROCEDURES TER VERSTERKING VAN DE RECHTSTREEKSE SAMENWERKING MET SERVICEPROVIDERS EN ENTITEITEN OP HET GRONDGEBIED VAN EEN ANDERE PARTIJ

Artikel 6

– Verzoek om domeinnaamregistratie-informatie

1. Iedere partij stelt de nodige wetgevende en andere maatregelen vast om haar bevoegde autoriteiten in het kader van specifieke strafrechtelijke onderzoeken of procedures de bevoegdheid te verlenen een entiteit die op het grondgebied van een andere partij domeinnaamregistratiediensten aanbiedt, te verzoeken informatie te verstrekken die in haar bezit is of tot toegang waartoe zij gerechtigd is, teneinde de registrant van een domeinnaam te identificeren of met die registrant contact op te nemen.

2. Iedere partij stelt de nodige wetgevende en andere maatregelen vast om een entiteit op haar grondgebied toe te staan dergelijke informatie te verstrekken naar aanleiding van een verzoek uit hoofde van lid 1, met inachtneming van redelijke voorwaarden waarin het nationale recht voorziet.

3. In het in lid 1 bedoelde verzoek wordt vermeld:
a. de datum waarop het verzoek is gedaan en de identiteit en de contactgegevens van de bevoegde autoriteit die het verzoek heeft gedaan;
b. de domeinnaam waarover informatie wordt gevraagd en een gedetailleerde lijst van de gevraagde informatie, met vermelding van de specifieke gegevenselementen;
c. een verklaring dat het verzoek op grond van dit protocol wordt gedaan, dat de informatie nodig is vanwege het belang ervan voor een bepaald strafrechtelijk onderzoek of een specifieke strafrechtelijke procedure en dat de informatie alleen voor dat specifieke strafrechtelijk onderzoek of die specifieke strafprocedure zal worden gebruikt; en
d. de termijn waarbinnen en de wijze waarop de informatie openbaar moet worden gemaakt, alsmede eventuele andere bijzondere procedurele instructies.

4. Indien de instantie daarmee instemt, kan een partij een verzoek uit hoofde van lid 1 in elektronische vorm indienen. Er kan een passend niveau van beveiliging en authenticatie worden vereist.

5. Indien een entiteit als in lid 1 beschreven geen medewerking verleent, kan de verzoekende partij de entiteit verzoeken te motiveren waarom zij de gevraagde informatie niet verstrekt. De verzoekende partij kan verzoeken om overleg met de partij waar de entiteit is gevestigd, teneinde vast te stellen welke maatregelen getroffen kunnen worden om de informatie te verkrijgen.

6. Iedere partij deelt bij de ondertekening van het protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring, of op enig ander tijdstip, de secretaris-generaal van de Raad van Europa de namen en adressen mee van de autoriteiten die voor het in lid 5 bedoelde overleg zijn aangewezen.

7. De secretaris-generaal van de Raad van Europa stelt een register op van de uit hoofde van lid 6 door de partijen aangewezen autoriteiten en houdt dit bij. Iedere partij zorgt ervoor dat de in het register vermelde gegevens te allen tijde juist zijn.

Artikel 7

– Verstrekking van abonnee-informatie

1. Iedere partij stelt de nodige wetgevende en andere maatregelen vast om haar bevoegde autoriteiten de bevoegdheid te verlenen een bevel uit te vaardigen dat rechtstreeks gericht is tot een serviceprovider op het grondgebied van een andere partij, teneinde die serviceprovider gespecificeerde door hem opgeslagen abonnee-informatie te doen verstrekken die in zijn bezit is of tot toegang waartoe hij gerechtigd is, indien die abonnee-informatie nodig is voor specifieke strafrechtelijke onderzoeken of strafprocedures van de uitvaardigende partij.

2. a) Iedere partij stelt de wetgevende en andere maatregelen vast die noodzakelijk zijn voor de verstrekking van abonnee-informatie door een serviceprovider op haar grondgebied naar aanleiding van een verzoek uit hoofde van lid 1.
b) Bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring kan een partij – met betrekking tot bevelen aan serviceproviders op haar grondgebied – de volgende verklaring afleggen: „Het bevel uit hoofde van artikel 7, lid 1, moet worden uitgevaardigd door of onder toezicht van een aanklager of een andere justitiële autoriteit, of anderszins onder onafhankelijk toezicht worden uitgevaardigd."

3. In het in lid 1 bedoelde bevel wordt vermeld:
a. de uitvaardigende autoriteit en de datum van uitvaardiging;
b. een verklaring dat het bevel uit hoofde van dit protocol is uitgevaardigd;
c. de naam en het adres van de serviceprovider(s) aan wie het bevel moet worden betekend;
d. de strafbare feiten waarop het strafrechtelijk onderzoek of de strafprocedure betrekking heeft;
e. de autoriteit die de specifieke abonnee-informatie opvraagt, indien dat niet de uitvaardigende autoriteit is; en
f. een gedetailleerde beschrijving van de gevraagde specifieke abonnee-informatie.

4. Het in lid 1 bedoelde bevel gaat vergezeld van de volgende aanvullende informatie:
a. de nationale rechtsgrondslagen uit hoofde waarvan de autoriteit bevoegd is het bevel uit te vaardigen;
b. een verwijzing naar de wettelijke bepalingen en de toepasselijke straffen voor het strafbaar feit dat wordt onderzocht of vervolgd;
c. de contactgegevens van de autoriteit waaraan de serviceprovider de abonnee-informatie moet toezenden, die hij om nadere informatie kan verzoeken of waaraan hij anderszins antwoord moet geven;
d. de termijn waarbinnen en de wijze waarop de abonnee-informatie moeten worden toegezonden;
e. of reeds om bewaring van de gegevens is verzocht, met opgave van de bewaringsdatum en eventuele toepasselijke referentienummers;
f. eventuele bijzondere procedurele instructies;
g. indien van toepassing, een verklaring dat de gelijktijdige kennisgeving overeenkomstig lid 5 heeft plaatsgevonden; en
h. alle andere informatie die van nut kan zijn om de verstrekking van de abonnee-informatie te verkrijgen.

5. a. Een partij kan, bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring, en op enig ander tijdstip, de secretaris-generaal van de Raad van Europa ervan kennisgeving doen dat wanneer een bevel overeenkomstig lid 1 is uitgevaardigd aan een serviceprovider op haar grondgebied, de partij, in alle gevallen dan wel in bepaalde omstandigheden, verlangt dat gelijktijdig kennis wordt gegeven van het bevel, de aanvullende informatie en een samenvatting van de feiten in verband met het onderzoek of de procedure.
b. Ongeacht of een partij een kennisgeving uit hoofde van lid 5, punt a), verlangt, kan zij van de serviceprovider verlangen dat deze de autoriteiten van de partij in bepaalde omstandigheden raadpleegt voorafgaand aan de verstrekking.
c. De overeenkomstig lid 5, punt a), in kennis gestelde of overeenkomstig lid 5, punt b), geraadpleegde autoriteiten kunnen de serviceprovider onverwijld opdracht geven de abonnee-informatie niet te verstrekken indien:
   i. de verstrekking strafrechtelijke onderzoeken of strafprocedures in die partij in gevaar kan brengen; of
   ii. de voorwaarden of gronden voor weigering uit hoofde van artikel 25, lid 4, en artikel 27, lid 4, van het verdrag van toepassing zouden zijn indien de abonnee-informatie via wederzijdse bijstand was opgevraagd.
d. De overeenkomstig lid 5, punt a), in kennis gestelde of overeenkomstig lid 5, punt b), geraadpleegde autoriteiten:
   i. kunnen de in lid 4, punt c), bedoelde autoriteit ten behoeve van de toepassing van lid 5, punt c), om aanvullende informatie verzoeken en verstrekken deze informatie niet zonder toestemming van die autoriteit aan de serviceprovider; en
   ii. stellen de in lid 4, punt c), bedoelde autoriteit onverwijld in kennis indien de serviceprovider opdracht heeft gekregen de abonnee-informatie niet te verstrekken, en geven de redenen daarvoor op.

e. Een partij wijst één autoriteit aan voor het in ontvangst nemen van kennisgevingen overeenkomstig lid 5, punt a), en het uitvoeren van de maatregelen omschreven in lid 5, punten b), c) en d). Wanneer de partij voor de eerste maal overeenkomstig lid 5, punt a), kennisgeving doet aan de secretaris-generaal van de Raad van Europa, deelt zij de secretaris-generaal de contactgegevens van die autoriteit mee.
f. De secretaris-generaal van de Raad van Europa zet een register op van de uit hoofde van lid 5, punt e), door de partijen aangewezen autoriteiten en houdt dit bij, en registreert of en zo ja, wanneer kennisgeving is vereist overeenkomstig lid 5, punt a). Iedere partij zorgt ervoor dat de in het register vermelde gegevens te allen tijde juist zijn.

6. Indien dit voor de serviceprovider aanvaardbaar is, kan een partij bevelen uit hoofde van lid 1 en aanvullende informatie als bedoeld in lid 4 in elektronische vorm indienen. Een partij kan de in lid 5 bedoelde kennisgeving en aanvullende informatie in elektronische vorm verstrekken. Er kan een passend niveau van beveiliging en authenticatie worden vereist.

7. Indien een serviceprovider de in lid 4, punt c), bedoelde autoriteit meedeelt dat hij de gevraagde abonnee-informatie niet zal verstrekken, of indien hij naar aanleiding van het in lid 1 bedoelde bevel geen abonnee-informatie verstrekt binnen dertig dagen na ontvangst van het bevel of binnen de in lid 4, punt d), vastgestelde termijn, indien deze langer is, kunnen de bevoegde autoriteiten van de uitvaardigende partij het bevel uitsluitend via artikel 8 of andere vormen van wederzijdse bijstand ten uitvoer leggen. Partijen kunnen verlangen dat een serviceprovider de reden vermeldt voor zijn weigering de in het bevel gevraagde abonnee-informatie te verstrekken.

8. Een partij kan, bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring, verklaren dat een uitvaardigende partij de serviceprovider moet verzoeken om verstrekking van abonnee-informatie alvorens actie te ondernemen om deze informatie overeenkomstig artikel 8 te verkrijgen, tenzij de uitvaardigende partij een redelijke verklaring geeft waarom zij dit niet heeft gedaan.

9. Bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring kan een partij:
a. zich het recht voorbehouden dit artikel niet toe te passen; of
b. indien verstrekking van bepaalde soorten toegangsnummers uit hoofde van dit artikel in strijd zou zijn met de grondbeginselen van haar nationale rechtsstelsel, zich het recht voorbehouden dit artikel niet op dergelijke nummers toe te passen.

AFDELING 3 – PROCEDURES TER VERSTERKING VAN DE INTERNATIONALE SAMENWERKING TUSSEN AUTORITEITEN BIJ DE VERSTREKKING VAN OPGESLAGEN COMPUTERGEGEVENS

Artikel 8

– Uitvoering geven aan bevelen van een andere partij om abonnee-informatie en verkeersgegevens met spoed te verstrekken

1. Iedere partij stelt de nodige wetgevende en andere maatregelen vast om haar bevoegde autoriteiten de bevoegdheid te verlenen een bevel uit te vaardigen dat in het kader van een verzoek bij een andere partij wordt ingediend teneinde een serviceprovider op het grondgebied van de aangezochte partij te verplichten tot verstrekking van gespecificeerde opgeslagen
a. abonnee-informatie, en
b. verkeersgegevens
die in het bezit zijn van die serviceprovider of tot toegang waartoe die serviceprovider gerechtigd is, indien die gegevens noodzakelijk zijn voor een specifiek strafrechtelijk onderzoek of een specifieke strafprocedure van de partij.

2. Iedere partij stelt de nodige wetgevende en andere maatregelen vast om uitvoering te geven aan een door een verzoekende partij krachtens lid 1 ingediend bevel.

3. In haar verzoek dient de verzoekende partij het in lid 1 bedoelde bevel, de ondersteunende informatie en eventuele bijzondere procedurele instructies in bij de aangezochte partij.
a. In het bevel worden de volgende gegevens vermeld:
   i. de uitvaardigende autoriteit en de datum van uitvaardiging van het bevel;
   ii. een verklaring dat het bevel uit hoofde van dit protocol wordt ingediend;
   iii. de naam en het adres van de serviceprovider(s) aan wie het bevel moet worden betekend;
   iv. de strafbare feiten waarop het strafrechtelijk onderzoek of de strafprocedure betrekking heeft;
   v. de autoriteit die de informatie of de gegevens opvraagt, indien dat niet de uitvaardigende autoriteit is; en
   vi. een gedetailleerde beschrijving van de gevraagde specifieke informatie of gegevens.

b. In de ondersteunende informatie, die wordt verstrekt om de aangezochte partij te helpen uitvoering te geven aan het bevel en die niet zonder toestemming van de verzoekende partij aan de serviceprovider mag worden verstrekt, wordt het volgende vermeld:
   i. de nationale rechtsgrondslagen uit hoofde waarvan de autoriteit bevoegd is het bevel uit te vaardigen;
   ii. de wettelijke bepalingen en de toepasselijke straffen voor het strafbaar feit dat wordt onderzocht of vervolgd;
   iii. de reden waarom de verzoekende partij van mening is dat de serviceprovider in het bezit is van de gegevens of gerechtigd is tot toegang daartoe;
   iv. een samenvatting van de feiten in verband met het onderzoek of de procedure;
   v. de relevantie van de informatie of gegevens voor het onderzoek of de procedure;
   vi. de contactgegevens van de autoriteit of autoriteiten die nadere informatie kunnen verstrekken;
   vii. of reeds om bewaring van de informatie of gegevens is verzocht, met opgave van de bewaringsdatum en eventuele toepasselijke referentienummers; en
   viii. of de informatie of de gegevens al op andere wijze zijn opgevraagd, en zo ja, op welke wijze.
c. De verzoekende partij kan de aangezochte partij verzoeken bijzondere procedurele instructies uit te voeren.

4. Een partij kan bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring en op enig ander tijdstip verklaren dat aanvullende ondersteunende informatie vereist is om uitvoering te gegeven aan bevelen als bedoeld in lid 1.

5. De aangezochte partij aanvaardt verzoeken in elektronische vorm. Zij mag een passend niveau van beveiliging en authenticatie vereisen alvorens het verzoek te aanvaarden.

6. a. Vanaf de datum waarop de aangezochte partij alle in de leden 3 en 4 genoemde informatie heeft ontvangen, levert zij redelijke inspanningen om de serviceprovider binnen vijfenveertig dagen, zo niet eerder, van dienst te zijn, en gelast zij de toezending van de gevraagde informatie of gegevens binnen:
   i. twintig dagen voor abonnee-informatie; en
   ii. vijfenveertig dagen voor verkeersgegevens.
b. De aangezochte partij zorgt ervoor dat de te verstrekken informatie of gegevens onverwijld aan de verzoekende partij worden toegezonden.

7. Indien de aangezochte partij de in lid 3, punt c), bedoelde instructies niet op de gevraagde wijze kan opvolgen, stelt zij de verzoekende partij daarvan onverwijld in kennis en geeft zij, indien van toepassing, aan onder welke voorwaarden zij aan het verzoek zou kunnen voldoen, waarna de verzoekende partij bepaalt of het verzoek toch moet worden uitgevoerd.

8. De aangezochte partij mag weigeren een verzoek uit te voeren op de gronden die zijn vastgesteld in artikel 25, lid 4, of artikel 27, lid 4, van het verdrag, of kan voorwaarden opleggen die zij noodzakelijk acht om uitvoering van het verzoek mogelijk te maken. De aangezochte partij mag de uitvoering van verzoeken uitstellen om redenen die uit hoofde van artikel 27, lid 5, van het verdrag zijn vastgesteld. De aangezochte partij stelt de verzoekende partij zo spoedig mogelijk in kennis van de weigering, de voorwaarden of het uitstel. De aangezochte partij stelt de verzoekende partij tevens in kennis van andere omstandigheden die de uitvoering van het verzoek aanzienlijk kunnen vertragen. Artikel 28, lid 2, punt b), van het verdrag is van toepassing op dit artikel.

9. a. Indien de verzoekende partij niet kan voldoen aan een door de aangezochte partij uit hoofde van lid 8 opgelegde voorwaarde, stelt zij de aangezochte partij daarvan onverwijld in kennis. De aangezochte partij bepaalt vervolgens of de informatie of het materiaal toch moet worden verstrekt.
b. Indien de verzoekende partij de voorwaarde aanvaardt, is zij daardoor gebonden. Een aangezochte partij die informatie of materiaal verstrekt waarvoor een dergelijke voorwaarde geldt, kan van de verzoekende partij, met betrekking tot die voorwaarde, nadere uitleg verlangen omtrent het gebruik dat van deze informatie of van dit materiaal is gemaakt.

10. Iedere partij deelt bij de ondertekening van het protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring de secretaris-generaal van de Raad van Europa de contactgegevens en alle wijzigingen daarvan mee van de autoriteiten die zijn aangewezen:
a. voor het indienen van een bevel krachtens dit artikel; en
b. voor het in ontvangst nemen van een bevel uit hoofde van dit artikel.

11. Een partij kan bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring verklaren dat zij verlangt dat verzoeken van andere partijen uit hoofde van dit artikel bij haar worden ingediend door de centrale autoriteit van de verzoekende partij of door een andere autoriteit die in onderling overleg door de betrokken partijen is vastgesteld.

12. De secretaris-generaal van de Raad van Europa stelt een register op van de uit hoofde van lid 10 door de partijen aangewezen autoriteiten en houdt dit bij. Iedere partij zorgt ervoor dat de voor opname in het register verstrekte gegevens te allen tijde juist zijn.

13. Bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring kan een partij zich het recht voorbehouden dit artikel niet toe te passen op verkeersgegevens.

Artikel 9

– Spoedverstrekking van opgeslagen computergegevens in een noodsituatie

1. a. Iedere partij stelt de wetgevende en andere maatregelen vast die in een noodsituatie nodig kunnen zijn om haar contactpunt voor het 24/7 netwerk als bedoeld in artikel 35 van het verdrag (hierna „contactpunt") in staat te stellen om, zonder een verzoek om wederzijdse bijstand, een verzoek door te zenden naar en te ontvangen van een contactpunt in een andere partij dat onmiddellijke bijstand vraagt om van een serviceprovider op het grondgebied van die partij spoedverstrekking te verkrijgen van gespecificeerde opgeslagen computergegevens die in het bezit zijn van die serviceprovider of tot toegang waartoe die serviceprovider gerechtigd is.
b. Een partij kan bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring verklaren dat zij geen gevolg zal geven aan verzoeken als bedoeld in lid 1, punt a), die uitsluitend de verstrekking van abonnee-informatie betreffen.

2. Iedere partij stelt de nodige wetgevende en andere maatregelen vast om uit hoofde van lid 1:
a. haar autoriteiten in staat te stellen naar aanleiding van een verzoek uit hoofde van lid 1 gegevens op te vragen bij een serviceprovider op haar grondgebied;
b. een serviceprovider op haar grondgebied in staat te stellen de gevraagde gegevens te verstrekken aan haar autoriteiten naar aanleiding van een verzoek uit hoofde van lid 2, punt a); en
c. haar autoriteiten in staat te stellen de gevraagde gegevens aan de verzoekende partij te verstrekken.

3. In het in lid 1 bedoelde verzoek wordt vermeld:
a. de bevoegde autoriteit die de gegevens opvraagt en de datum waarop het verzoek is gedaan;
b. een verklaring dat het verzoek krachtens dit protocol is uitgevaardigd;
c. de naam en het adres van de serviceprovider of serviceproviders die in het bezit is of zijn van de gevraagde gegevens of tot toegang daartoe gerechtigd is of zijn;
d. het strafbare feit of de strafbare feiten die het voorwerp uitmaken van het strafrechtelijk onderzoek of de strafprocedure en een verwijzing naar de wettelijke bepalingen en toepasselijke straffen;
e. voldoende feiten om aan te tonen dat er sprake is van een noodsituatie en aan te geven wat het verband is met de gevraagde gegevens;
f. een gedetailleerde beschrijving van de gevraagde gegevens;
g. eventuele bijzondere procedurele instructies; en
h. alle andere informatie die van nut kan zijn om de verstrekking van de gevraagde gegevens te verkrijgen.

4. De aangezochte partij aanvaardt verzoeken in elektronische vorm. Een partij kan ook mondeling verzonden verzoeken aanvaarden en kan bevestiging in elektronische vorm verlangen. Zij kan een passend niveau van beveiliging en authenticatie vereisen alvorens een verzoek te aanvaarden.

5. Een partij kan bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring verklaren dat zij verzoekende partijen, na de uitvoering van het verzoek, ertoe verplicht het verzoek en alle ter ondersteuning daarvan verstrekte aanvullende informatie in te dienen in een formaat en via een kanaal zoals bepaald door de aangezochte partij, mogelijk in het kader van wederzijdse bijstand.

6. De aangezochte partij stelt de verzoekende partij met spoed in kennis van haar beslissing betreffende het in lid 1 bedoelde verzoek en geeft, indien van toepassing, aan onder welke voorwaarden zij de gegevens zou verstrekken en welke andere vormen van samenwerking er eventueel beschikbaar zijn.

7. a. Indien de verzoekende partij niet kan voldoen aan een door de aangezochte partij uit hoofde van lid 6 opgelegde voorwaarde, stelt zij de aangezochte partij daarvan onverwijld in kennis. De aangezochte partij bepaalt vervolgens of de informatie of het materiaal toch moet worden verstrekt. b) Indien de verzoekende partij de voorwaarde aanvaardt, is zij daardoor gebonden.

b. Een aangezochte partij die informatie of materiaal verstrekt waarvoor een dergelijke voorwaarde geldt, kan van de verzoekende partij, met betrekking tot die voorwaarde, nadere uitleg verlangen omtrent het gebruik dat van deze informatie of van dit materiaal is gemaakt.

AFDELING 4 – PROCEDURES VOOR WEDERZIJDSE BIJSTAND IN NOODSITUATIES

Artikel 10

– Wederzijdse bijstand in noodsituaties

1. Iedere partij kan om snelle wederzijdse bijstand verzoeken wanneer zij van mening is dat er sprake is van een noodsituatie. Een verzoek uit hoofde van dit artikel vermeldt, naast de andere vereiste inhoud, een beschrijving van de feiten die aantonen dat er sprake is van een noodsituatie en wat het verband is met de gevraagde bijstand.

2. De aangezochte partij aanvaardt dergelijke verzoeken in elektronische vorm. De aangezochte partij mag een passend niveau van beveiliging en authenticatie vereisen alvorens het verzoek te aanvaarden.

3. De aangezochte partij kan met spoed aanvullende informatie opvragen om het verzoek te kunnen beoordelen. De verzoekende partij verstrekt deze aanvullende informatie met spoed.

4. Zodra de aangezochte partij zich ervan heeft vergewist dat er sprake is van een noodsituatie en aan de andere vereisten voor wederzijdse bijstand is voldaan, beantwoordt zij met spoed het verzoek.

5. Iedere partij zorgt ervoor dat er bij haar centrale autoriteit, of bij andere autoriteiten die verantwoordelijk zijn voor het beantwoorden van verzoeken om wederzijdse bijstand, vierentwintig uur per dag en zeven dagen per week iemand beschikbaar is voor het beantwoorden van verzoeken uit hoofde van dit artikel.

6. De centrale autoriteit of andere voor wederzijdse bijstand verantwoordelijke autoriteiten van de verzoekende en de aangezochte partij kunnen onderling bepalen dat de resultaten van de uitvoering van een verzoek uit hoofde van dit artikel, of een voorlopige versie daarvan, aan de verzoekende partij kunnen worden verstrekt via een ander kanaal dan het voor het verzoek gebruikte kanaal.

7. Wanneer er tussen de verzoekende en de aangezochte partij geen verdrag inzake wederzijdse bijstand noch een regeling op basis van uniforme of wederkerige wetgeving van kracht is, zijn artikel 27, lid 2, punt b), en de leden 3 tot en met 8, alsmede artikel 28, leden 2 tot en met 4, van het verdrag van toepassing op dit artikel.

8. Indien er wel een dergelijk verdrag of een dergelijke regeling bestaat, wordt dit artikel aangevuld met de bepalingen van dat verdrag of die regeling, tenzij de betrokken partijen onderling besluiten in plaats daarvan een of meer van de in lid 7 van dit artikel bedoelde bepalingen van het verdrag toe te passen.

9. Iedere partij kan bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring verklaren dat verzoeken ook rechtstreeks kunnen worden gericht aan haar gerechtelijke autoriteiten, via de kanalen van de Internationale Criminele Politieorganisatie (Interpol) of haar 24/7-contactpunt dat is ingesteld krachtens artikel 35 van het verdrag. In een dergelijk geval wordt tegelijkertijd door tussenkomst van de centrale autoriteit van de verzoekende partij een afschrift gezonden aan de centrale autoriteit van de aangezochte partij. Wanneer een verzoek rechtstreeks naar een justitiële autoriteit van de aangezochte partij is gezonden en die autoriteit niet bevoegd is om het verzoek te behandelen, zendt deze het verzoek door naar de bevoegde nationale autoriteit en stelt zij de verzoekende partij daarvan rechtstreeks op de hoogte.

AFDELING 5 – PROCEDURES INZAKE INTERNATIONALE SAMENWERKING BIJ GEBREKE VAN TOEPASSELIJKE INTERNATIONALE OVEREENKOMSTEN

Artikel 11

– Videoconferentie

1. Een verzoekende partij kan erom vragen dat getuigenverklaringen en verklaringen van deskundigen door middel van een videoconferentie worden afgenomen, en de aangezochte partij kan dat toestaan. De verzoekende partij en de aangezochte partij plegen overleg om een oplossing voor eventuele problemen in verband met de uitvoering van het verzoek te faciliteren, bijvoorbeeld met betrekking tot: de vraag welke partij als voorzitter optreedt; de autoriteiten en personen die aanwezig zullen zijn; de vraag of een of beide partijen een bepaalde eed afleggen, waarschuwingen uitspreken of instructies geven aan een getuige of deskundige; de wijze waarop de getuige of deskundige wordt gehoord; de wijze waarop de rechten van de getuige of deskundige worden verzekerd; de behandeling van aanspraken op voorrechten of immuniteiten; de behandeling

van bezwaren tegen vragen of antwoorden; en de vraag of een van de partijen dan wel beide partijen diensten op het gebied van vertaling, vertolking en transcriptie aanbieden.

2. a. De centrale autoriteiten van de aangezochte en de verzoekende partij communiceren voor de toepassing van dit artikel rechtstreeks met elkaar. De aangezochte partij kan dergelijke verzoeken in elektronische vorm aanvaarden. Zij mag een passend niveau van beveiliging en authenticatie vereisen alvorens het verzoek te aanvaarden.
b. De aangezochte partij deelt de verzoekende partij mee waarom zij het verzoek niet uitvoert of de uitvoering ervan uitstelt. Artikel 27, lid 8, van het verdrag is van toepassing op dit artikel. Onverminderd andere voorwaarden die een aangezochte partij overeenkomstig dit artikel kan stellen, zijn de leden 2 tot en met 4 van artikel 28 van het verdrag van toepassing op dit artikel.

3. Een aangezochte partij die uit hoofde van dit artikel bijstand verleent, spant zich in om te bewerkstelligen dat de persoon wiens getuigenis of verklaring wordt gevraagd, aanwezig is. In voorkomend geval kan de aangezochte partij, voor zover haar recht dit toelaat, de nodige maatregelen nemen om een getuige of deskundige te verplichten op een bepaald tijdstip en op een bepaalde plaats in de aangezochte partij te verschijnen.

4. De door de verzoekende partij gespecificeerde procedures voor het houden van de videoconferentie worden gevolgd, tenzij dat onverenigbaar is met het nationale recht van de aangezochte partij. In geval van onverenigbaarheid of voor zover de procedure niet door de verzoekende partij is gespecificeerd, past de aangezochte partij de procedure uit hoofde van haar nationale recht toe, tenzij de verzoekende en de aangezochte partij onderling anders bepalen.

5. Indien de getuige of deskundige tijdens de videoconferentie:
a. een opzettelijk onjuiste verklaring aflegt, terwijl die persoon overeenkomstig het nationale recht van de aangezochte partij ertoe verplicht is een waarheidsgetrouwe verklaring af te leggen,
b. weigert een verklaring af te leggen, terwijl die persoon overeenkomstig het nationale recht van de aangezochte partij ertoe verplicht een verklaring af te leggen, of
c. zich in de loop van de procedure schuldig maakt aan andere misdragingen die krachtens het nationale recht van de aangezochte partij verboden zijn,
is die persoon in de aangezochte partij strafbaar op dezelfde wijze als wanneer de genoemde gedraging in het kader van een binnenlandse procedure had plaatsgevonden, zulks onverminderd de rechtsbevoegdheid krachtens het nationale recht van de verzoekende partij.

6. a. Tenzij de verzoekende partij en de aangezochte partij onderling anders zijn overeengekomen, draagt de aangezochte partij alle kosten in verband met de uitvoering van een verzoek uit hoofde van dit artikel, met uitzondering van:
i. honoraria van getuigen-deskundigen;
ii. kosten van vertaling, vertolking en transcriptie; en
iii. buitengewone kosten.
b. Indien de uitvoering van een verzoek tot buitengewone kosten zou leiden, plegen de verzoekende partij en de aangezochte partij overleg om te bepalen onder welke voorwaarden het verzoek kan worden uitgevoerd.

7. Indien de verzoekende partij en de aangezochte partij zulks onderling overeenkomen:
a. kunnen de bepalingen van dit artikel worden toegepast voor de uitvoering van audioconferenties;
b. kan videoconferentietechnologie worden gebruikt voor andere dan de in lid 1 beschreven doeleinden of hoorzittingen, waaronder de identificatie van personen of voorwerpen.

8. Indien een aangezochte partij ervoor kiest het horen van een verdachte of beklaagde toe te staan, kan zij bijzondere voorwaarden en waarborgen vereisen met betrekking tot het afnemen van een getuigenis of verklaring van die persoon, het verstrekken van kennisgevingen aan die persoon of het toepassen van procedurele maatregelen ten aanzien van die persoon.

Artikel 12

– Gemeenschappelijke onderzoeksteams en gezamenlijke onderzoeken

1. In onderlinge overeenstemming kunnen de bevoegde autoriteiten van twee of meer partijen, wanneer versterkte coördinatie van bijzonder nut wordt geacht, op hun grondgebied gemeenschappelijke onderzoeksteams instellen en beheren, teneinde strafrechtelijke onderzoeken en strafprocedures te faciliteren. De respectieve betrokken partijen bepalen welke de bevoegde autoriteiten zijn.

2. De procedures en de voorwaarden voor de werking van gemeenschappelijke onderzoeksteams, zoals de specifieke doelstellingen, de samenstelling, de functies, de duur van de onderzoeksactiviteiten en eventuele verlengingstermijnen, de locatie, de organisatie, de voorwaarden voor het vergaren, doorgeven en gebruiken van informatie en bewijsmateriaal, de vertrouwelijkheidsvoorwaarden en de voorwaarden voor de be-

trokkenheid van de deelnemende autoriteiten van een partij bij onderzoeksactiviteiten die op het grondgebied van een andere partij plaatsvinden, worden door de bevoegde autoriteiten overeengekomen.

3. Een partij kan bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring verklaren dat haar centrale autoriteit de overeenkomst tot oprichting van het team moet ondertekenen of er anderszins mee moet instemmen.

4. De bevoegde en deelnemende autoriteiten communiceren rechtstreeks met elkaar, met dien verstande dat de partijen onderling afspraken kunnen maken over andere passende communicatiekanalen, wanneer uitzonderlijke omstandigheden meer centrale coördinatie vereisen.

5. Wanneer onderzoeksmaatregelen op het grondgebied van een van de betrokken partijen moeten worden uitgevoerd, kunnen de deelnemende autoriteiten van die partij hun eigen autoriteiten verzoeken deze maatregelen uit te voeren en is het niet noodzakelijk dat de andere partijen een verzoek om wederzijdse bijstand indienen. Deze maatregelen worden door de autoriteiten van die partij op haar grondgebied uitgevoerd onder de voorwaarden die krachtens het nationale recht van toepassing zijn op nationale onderzoeken.

6. Het gebruik van informatie die of bewijsmateriaal dat door de deelnemende autoriteiten van een partij aan de deelnemende autoriteiten van andere betrokken partijen is verstrekt, kan worden geweigerd of beperkt op de wijze die is uiteengezet in de in de leden 1 en 2 beschreven overeenkomst. Indien in die overeenkomst geen voorwaarden zijn vermeld voor het weigeren of beperken van het gebruik, kunnen de partijen gebruikmaken van de verstrekte informatie of het verstrekte bewijsmateriaal:

a. voor de doeleinden waarvoor de overeenkomst is gesloten;
b. voor het opsporen, onderzoeken en vervolgen van andere strafbare feiten dan die waarvoor de overeenkomst is gesloten, met voorafgaande toestemming van de autoriteiten die de informatie of het bewijsmateriaal hebben verstrekt. Toestemming is echter niet vereist wanneer fundamentele rechtsbeginselen van de partij die de informatie of het bewijsmateriaal gebruikt, vereisen dat zij de informatie of het bewijsmateriaal verstrekt ter bescherming van de rechten van een beklaagde in een strafprocedure. In dat geval stellen die autoriteiten de autoriteiten die de informatie of het bewijs hebben verstrekt, daarvan onverwijld in kennis; of
c. om een noodsituatie te voorkomen. In dat geval stellen de deelnemende autoriteiten die de informatie of het bewijs hebben ontvangen, de deelnemende autoriteiten die de informatie of het bewijs hebben verstrekt, daarvan onverwijld in kennis, tenzij onderling anders is overeengekomen.

7. Bij gebreke van een overeenkomst als beschreven in de leden 1 en 2, kunnen op onderling overeengekomen voorwaarden per geval gezamenlijke onderzoeken worden ingesteld. Dit lid is van toepassing ongeacht of er sprake is van een verdrag of regeling inzake wederzijdse bijstand op basis van uniforme of wederkerige wetgeving tussen de betrokken partijen.

HOOFDSTUK III – VOORWAARDEN EN WAARBORGEN

Artikel 13

– Voorwaarden en waarborgen

Overeenkomstig artikel 15 van het verdrag ziet iedere partij erop toe dat de invoering, uitwerking en toepassing van de in dit protocol bedoelde bevoegdheden en procedures onderworpen zijn aan de voorwaarden en waarborgen vervat in haar nationale recht, dat een passende bescherming moet bieden aan de rechten en vrijheden van de mens.

Artikel 14

– Bescherming van persoonsgegevens

1. Toepassingsgebied

a. Tenzij anders bepaald in de punten b) en c), verwerkt iedere partij de persoonsgegevens die zij uit hoofde van dit protocol ontvangt in overeenstemming met de leden 2 tot en met 15 van dit artikel.
b. Indien ten tijde van de ontvangst van persoonsgegevens uit hoofde van dit protocol zowel de doorgevende partij als de ontvangende partij wederzijds gebonden zijn door een internationale overeenkomst tot vaststelling van een algemeen kader tussen die partijen voor de bescherming van persoonsgegevens, die van toepassing is op de doorgifte van persoonsgegevens met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten en waarin is bepaald dat de verwerking van persoonsgegevens in het kader van die overeenkomst in overeenstemming is met de vereisten van de gegevensbeschermingswetgeving van de betrokken partijen, zijn de bepalingen van die overeenkomst, wat maatregelen betreft die onder het toepassingsgebied van die overeenkomst vallen, van toepassing op persoonsgegevens die in het kader van het protocol zijn ontvangen, in plaats van de leden 2 tot en met 15, tenzij de betrokken partijen anders zijn overeengekomen.

c. Indien de doorgevende partij en de ontvangende partij niet wederzijds gebonden zijn door een overeenkomst als bedoeld in punt b), kunnen zij overeenkomen dat de doorgifte van persoonsgegevens in het kader van dit protocol kan plaatsvinden op basis van andere overeenkomsten of regelingen tussen de betrokken partijen in plaats van de leden 2 tot en met 15.
d. Iedere partij gaat ervan uit dat de verwerking van persoonsgegevens overeenkomstig de punten a) en b) voldoet aan de vereisten van haar rechtskader inzake de bescherming van persoonsgegevens voor internationale doorgiften van persoonsgegevens, en dat uit hoofde van dat rechtskader geen verdere toestemming voor doorgifte vereist is. Een partij mag de doorgifte van gegevens aan een andere partij in het kader van dit protocol alleen weigeren of verhinderen om redenen van gegevensbescherming onder de voorwaarden van lid 15, wanneer punt a) van toepassing is, of onder de voorwaarden van een overeenkomst als bedoeld in punt b) of c), indien een van die punten van toepassing is.
e. Niets in dit artikel belet een partij om strengere waarborgen toe te passen op de verwerking door haar eigen autoriteiten van in het kader van dit protocol ontvangen persoonsgegevens.

2. Doel en gebruik
a. Een partij die persoonsgegevens heeft ontvangen, verwerkt deze voor de in artikel 2 omschreven doeleinden. Zij verwerkt de persoonsgegevens niet verder voor een daarmee onverenigbaar doel en verwerkt de gegevens niet verder wanneer haar nationale rechtskader zulks niet toestaat. Dit artikel doet geen afbreuk aan de mogelijkheid voor de doorgevende partij om in een specifiek geval uit hoofde van dit protocol aanvullende voorwaarden op te leggen, maar dergelijke voorwaarden mogen geen algemene voorwaarden inzake gegevensbescherming inhouden.
b. De ontvangende partij ziet er overeenkomstig haar nationale rechtskader op toe dat de gevraagde en vervolgens verwerkte persoonsgegevens relevant zijn voor het doel van de verwerking en in verhouding daartoe niet bovenmatig zijn.

3. Kwaliteit en integriteit
Iedere partij neemt redelijke maatregelen om ervoor te zorgen dat persoonsgegevens worden bewaard en bijgewerkt met de nauwkeurigheid en volledigheid die voor de rechtmatige verwerking van de persoonsgegevens vereist en passend is, rekening houdend met de doeleinden waarvoor zij worden verwerkt.

4. Gevoelige gegevens
Een partij mag persoonsgegevens waaruit raciale of etnische afkomst, politieke opvattingen, godsdienstige of andere overtuigingen of het lidmaatschap van een vakvereniging blijken, genetische gegevens, biometrische gegevens die gezien de ermee gepaard gaande risico's als gevoelig worden beschouwd, en persoonsgegevens die gezondheid of seksueel gedrag betreffen, slechts verwerken met inachtneming van passende waarborgen ter voorkoming van het risico van ongerechtvaardigde nadelige gevolgen van het gebruik van dergelijke gegevens, en in het bijzonder ter voorkoming van onwettige discriminatie.

5. Bewaringstermijnen
Iedere partij bewaart persoonsgegevens niet langer dan nodig en passend is voor de doeleinden van de verwerking van de gegevens overeenkomstig lid 2. Om aan deze verplichting te voldoen, stelt zij in haar nationale rechtskader specifieke bewaringstermijnen vast of voorziet zij in periodieke toetsing van de noodzaak om gegevens langer te bewaren.

6. Geautomatiseerde besluiten
Besluiten die aanzienlijke nadelige gevolgen hebben voor de relevante belangen van de persoon op wie de persoonsgegevens betrekking hebben, mogen niet uitsluitend gebaseerd zijn op geautomatiseerde verwerking van persoonsgegevens, tenzij dat is toegestaan uit hoofde van het nationale recht en in passende waarborgen is voorzien, waaronder de mogelijkheid van menselijke tussenkomst.

7. Gegevensbeveiliging en beveiligingsincidenten
a. Iedere partij zorgt ervoor dat zij beschikt over passende technologische, fysieke en organisatorische maatregelen om persoonsgegevens te beschermen, met name tegen verlies of onopzettelijke of ongeoorloofde toegang, verspreiding, wijziging of vernietiging („beveiligingsincidenten").
b. Wanneer een veiligheidsincident aan het licht komt dat gepaard gaat met een aanzienlijk risico van fysiek letsel of niet-fysieke schade aan personen of aan de andere partij, beoordeelt de ontvangende partij onverwijld de waarschijnlijkheid en de omvang ervan en neemt zij onverwijld passende maatregelen om dergelijk letsel of dergelijke schade te beperken. Deze maatregelen houden onder meer in dat kennisgeving wordt gedaan aan de doorgevende autoriteit, dan wel, voor de toepassing van hoofdstuk II, afdeling 2, aan de autoriteit(en) die zijn aangewezen krachtens lid 7, punt c). In de kennisgeving kunnen echter ook passende beperkingen op verdere verspreiding van de kennisgeving worden opgenomen: verspreiding kan worden uitgesteld of achterwege blijven wanneer de kennisgeving de nationale veiligheid in gevaar kan brengen, of worden uitgesteld wanneer de kennisgeving de maatregelen ter bescherming van de openbare veiligheid in gevaar kan brengen. De maatregelen omvatten ook kennisgeving aan de betrokken persoon, tenzij de partij passende maatregelen heeft genomen waardoor er niet langer een aanzienlijk risico bestaat. De kennisgeving aan de betrokken persoon kan worden uitgesteld of achterwege blij-

ven onder de voorwaarden van lid 12, punt a), i). De in kennis gestelde partij kan verzoeken om overleg en aanvullende informatie over het incident en de respons erop.

c. Iedere partij stelt bij de ondertekening van het protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring de secretaris-generaal van de Raad van Europa in kennis van de autoriteit(en) waaraan uit hoofde van lid 7, punt b), kennisgeving moet worden gedaan voor de doeleinden van hoofdstuk II, afdeling 2; de verstrekte informatie kan later worden gewijzigd.

8. Bijhouden van bestanden

Iedere partij houdt bestanden bij of beschikt over andere passende middelen om aan te tonen hoe de persoonsgegevens van een persoon in een specifiek geval worden geraadpleegd, gebruikt en verstrekt.

9. Verdere uitwisseling binnen een partij

a. Wanneer een autoriteit van een partij persoonsgegevens die oorspronkelijk uit hoofde van dit protocol zijn ontvangen, aan een andere autoriteit van die partij verstrekt, verwerkt die andere autoriteit deze gegevens in overeenstemming met dit artikel, met inachtneming van lid 9, punt b).
b. Onverminderd lid 9, punt a), kan een partij die uit hoofde van artikel 17 een voorbehoud heeft gemaakt, door haar ontvangen persoonsgegevens verstrekken aan haar constituerende staten of vergelijkbare territoriale entiteiten, mits de partij maatregelen heeft getroffen om ervoor te zorgen dat de ontvangende autoriteiten de gegevens doeltreffend blijven beschermen door te voorzien in een niveau van bescherming van de gegevens dat vergelijkbaar is met dat waarin dit artikel voorziet.
c. Indien er aanwijzingen zijn van onjuiste toepassing van dit lid, kan de doorgevende partij verzoeken om overleg en relevante informatie over die aanwijzingen.

10. Verdere doorgifte naar een andere staat of internationale organisatie

a. De ontvangende partij mag de persoonsgegevens alleen doorgeven aan een andere staat of internationale organisatie indien daarvoor voorafgaande toestemming is verleend door de doorgevende autoriteit of, voor de toepassing van hoofdstuk II, afdeling 2, de overeenkomstig lid 10, punt b). aangewezen autoriteit(en).
b. Iedere partij stelt bij de ondertekening van het protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring de secretaris-generaal van de Raad van Europa in kennis van de autoriteiten die toestemming kunnen verlenen voor de toepassing van hoofdstuk II, afdeling 2; de verstrekte informatie kan later worden gewijzigd.

11. Transparantie en kennisgeving

a. Iedere partij stelt, door publicatie van algemene kennisgevingen of door een persoonlijke kennisgeving, de persoon wiens persoonsgegevens zijn verzameld, daarvan in kennis, met betrekking tot:
   i. de rechtsgrondslag en het doel van de verwerking;
   ii. alle bewaringstermijnen of toetsingstermijnen overeenkomstig lid 5, naargelang het geval;
   iii. ontvangers of categorieën ontvangers aan wie dergelijke gegevens worden verstrekt; en
   iv. toegang, rectificatie en de beschikbare rechtsmiddelen.
b. Een partij kan elke verplichting tot persoonlijke kennisgeving onderwerpen aan redelijke beperkingen uit hoofde van haar interne rechtskader overeenkomstig de voorwaarden van lid 12, punt a), i).
c. Wanneer het nationale rechtskader van de doorgevende partij vereist dat de persoon wiens gegevens aan een andere partij zijn verstrekt, daarvan persoonlijk in kennis wordt gesteld, neemt de doorgevende partij maatregelen om de andere partij op het tijdstip van de doorgifte in kennis te stellen van deze eis en passende contactgegevens te verstrekken. De persoonlijke kennisgeving wordt niet gedaan indien de andere partij heeft verzocht de verstrekking van de gegevens vertrouwelijk te behandelen, ingeval de voorwaarden voor beperkingen van lid 12, punt a), i), van toepassing zijn. Zodra deze beperkingen niet langer van toepassing zijn en de persoonlijke kennisgeving kan worden verstrekt, neemt de andere partij maatregelen om de doorgevende partij daarvan in kennis te stellen. Indien zij nog niet in kennis is gesteld, heeft de doorgevende partij het recht een verzoek in te dienen bij de ontvangende partij, die de doorgevende partij zal meedelen of de beperking al dan niet moet worden gehandhaafd.

12. Toegang en rectificatie

a. Iedere partij ziet erop toe dat eenieder wiens persoonsgegevens in het kader van dit protocol zijn ontvangen, het recht heeft om, in overeenstemming met de in haar interne rechtskader vastgestelde procedures, onverwijld:
   i. een schriftelijke of elektronische kopie te vragen en te verkrijgen van de documentatie die over die persoon wordt bewaard, met daarin de persoonsgegevens van de betrokkene, en de beschikbare informatie over de rechtsgrondslag en het doel van de verwerking, de bewaringstermijnen en de ontvangers of categorieën ontvangers van de gegevens (degenen die er „toegang" toe hebben), alsmede informatie over de beschikbare rechtsmiddelen; met dien verstande dat op de toegang in een bepaald geval op grond van het nationale rechtskader toegestane evenredige beperkingen van toepassing kunnen zijn die op het tijdstip van de uitspraak noodzakelijk zijn om de rechten en vrijheden van anderen of belangrijke doelstellingen van algemeen openbaar belang te beschermen en waarbij naar behoren rekening wordt gehouden met de legitieme belangen van de betrokkene;

ii) rectificatie wanneer de persoonsgegevens van de betrokkene onjuist zijn of onjuist zijn verwerkt; rectificatie omvat – indien dat passend en redelijk is, gezien de redenen voor rectificatie en de bijzondere context van de verwerking – correctie, aanvulling, wissing of anonimisering, beperking van de verwerking of afscherming.

b. Indien de toegang of rectificatie wordt geweigerd of beperkt, verstrekt de partij de betrokkene onverwijld in schriftelijke vorm, hetgeen tevens elektronisch kan geschieden, een antwoord waarmee de betrokkene in kennis wordt gesteld van de weigering of beperking. Dit antwoord vermeldt de gronden voor de weigering of beperking en verstrekt informatie over de beschikbare rechtsmiddelen. Alle kosten voor het verkrijgen van toegang moeten beperkt blijven tot wat redelijk is en mogen niet buitensporig zijn.

13. Gerechtelijke en buitengerechtelijke rechtsmiddelen
Iedere partij beschikt over doeltreffende gerechtelijke en buitengerechtelijke rechtsmiddelen om verhaal te zoeken tegen schendingen van dit artikel.

14. Toezicht
Iedere partij beschikt over een of meer overheidsinstanties die, alleen of cumulatief, onafhankelijke en effectieve toezichtstaken en -bevoegdheden uitoefenen met betrekking tot de in dit artikel genoemde maatregelen. De taken en bevoegdheden van deze instanties die alleen of cumulatief handelen, omvatten onderzoeksbevoegdheden, de bevoegdheid om naar aanleiding van klachten op te treden en het vermogen corrigerende maatregelen te nemen.

15. Raadpleging en opschorting
Een partij kan de doorgifte van persoonsgegevens aan een andere partij opschorten indien zij over substantieel bewijs beschikt waaruit blijkt dat de andere partij stelselmatig of wezenlijk inbreuk maakt op de voorwaarden van dit artikel of dat een wezenlijke inbreuk dreigt. Zij schort doorgiften niet op zonder een redelijke termijn in acht te nemen en niet eerder dan nadat de betrokken partijen gedurende een redelijke termijn overleg hebben kunnen plegen zonder dat zij tot een oplossing zijn gekomen. Een partij kan doorgiften echter voorlopig opschorten in geval van een stelselmatige of wezenlijke inbreuk die een aanzienlijk en imminent risico vormt voor het leven of de veiligheid van of voor aanzienlijke reputatieschade of financiële schade aan een natuurlijke persoon, in welk geval zij de andere partij onmiddellijk daarna in kennis stelt en overleg opent. Indien het overleg niet tot een oplossing heeft geleid, kan de andere partij de doorgiften wederkerig opschorten indien zij over substantieel bewijs beschikt dat de opschorting door de partij die tot opschorting is overgegaan, in strijd was met de bepalingen van dit lid. De partij die tot opschorting is overgegaan, heft de opschorting op zodra de inbreuk die de opschorting rechtvaardigde, is beëindigd; iedere wederkerige opschorting wordt op dat moment opgeheven. Persoonsgegevens die vóór de opschorting zijn doorgegeven, worden ook na de opschorting overeenkomstig het protocol behandeld.

HOOFDSTUK IV

– SLOTBEPALINGEN

Artikel 15

– Effecten van dit protocol

1. a. Artikel 39, lid 2, van het verdrag is van toepassing op dit protocol.
b. Partijen die lidstaten zijn van de Europese Unie, kunnen in hun wederzijdse betrekkingen het recht van de Europese Unie inzake de in dit protocol behandelde aangelegenheden toepassen.
c. Punt b) laat de volledige toepassing van dit protocol tussen partijen die lidstaten zijn van de Europese Unie en andere partijen onverlet.

2. Artikel 39, lid 3, van het verdrag is van toepassing op dit protocol.

Artikel 16

– Ondertekening en inwerkingtreding

1. Dit protocol staat open voor ondertekening door partijen bij het verdrag, die kunnen verklaren dat zij ermee instemmen erdoor gebonden te zijn, door:
a. te ondertekenen zonder voorbehoud van ratificatie, aanvaarding of goedkeuring; of
b. te ondertekenen met voorbehoud van ratificatie, aanvaarding of goedkeuring, gevolgd door ratificatie, aanvaarding of goedkeuring;

2. De akten van ratificatie, aanvaarding of goedkeuring worden neergelegd bij de secretaris-generaal van de Raad van Europa.

3. Dit protocol treedt in werking op de eerste dag van de maand die volgt op het verstrijken van een tijdvak van drie maanden na de datum waarop vijf partijen bij het verdrag, overeenkomstig de bepalingen van de leden 1 en 2 van dit artikel, hun instemming door het protocol te worden gebonden tot uitdrukking hebben gebracht.

4. Ten aanzien van iedere ondertekenende partij bij het verdrag die later zijn instemming door dit protocol te worden gebonden tot uitdrukking brengt, treedt het protocol in werking op de eerste dag van de maand die volgt op het verstrijken van een tijdvak van drie maanden na de datum waarop de partij haar instemming door het protocol te worden gebonden tot uitdrukking heeft gebracht overeenkomstig de leden 1 en 2 van dit artikel.

Artikel 17

– Federale clausule

1. Een federale staat kan zich het recht voorbehouden de verplichtingen ingevolge dit protocol aan te gaan voor zover deze in overeenstemming zijn met zijn fundamentele beginselen die ten grondslag liggen aan de betrekkingen tussen zijn centrale regering en de constituerende staten of andere vergelijkbare territoriale entiteiten, mits:
a. het protocol van toepassing is op de centrale regering van de federale staat;
b. een dergelijk voorbehoud geen afbreuk doet aan de verplichtingen om de door andere partijen gevraagde samenwerking aan te gaan overeenkomstig de bepalingen van hoofdstuk II; en
c. de bepalingen van artikel 13 van toepassing zijn op de constituerende staten of andere vergelijkbare territoriale entiteiten van de federale staat.

2. Een andere partij kan autoriteiten, serviceproviders of entiteiten op haar grondgebied beletten medewerking te verlenen naar aanleiding van een rechtstreeks verzoek of bevel van een constituerende staat of andere vergelijkbare territoriale entiteit van een federale staat die een voorbehoud heeft gemaakt als bedoeld in lid 1, tenzij die federale staat de secretaris- generaal van de Raad van Europa ervan in kennis stelt dat een constituerende staat of andere vergelijkbare territoriale entiteit de verplichtingen van dit protocol die op die federale staat van toepassing zijn, toepast. De secretaris-generaal van de Raad van Europa stelt een register op van dergelijke kennisgevingen en houdt dit bij.

3. Een andere partij belet autoriteiten, serviceproviders of entiteiten op haar grondgebied niet om op grond van een voorbehoud uit hoofde van lid 1 medewerking te verlenen aan een constituerende staat of andere vergelijkbare territoriale entiteit, indien via de centrale overheid een bevel of verzoek is ingediend of een overeenkomst inzake een gemeenschappelijk onderzoeksteam overeenkomstig artikel 12 is gesloten met medewerking van de centrale regering. In dergelijke situaties voorziet de centrale regering in de vervulling van de toepasselijke verplichtingen van het protocol, op voorwaarde dat met betrekking tot de bescherming van persoonsgegevens die aan de constituerende staten of vergelijkbare territoriale entiteiten worden verstrekt, slechts de voorwaarden van artikel 14, lid 9, of in voorkomend geval de voorwaarden van een overeenkomst of regeling als omschreven in artikel 14, lid l, punt b) of c), van toepassing zijn.

4. Ten aanzien van de bepalingen van dit protocol waarvan de toepassing onder de rechtsbevoegdheid valt van elk van de constituerende staten of andere vergelijkbare territoriale entiteiten die, ingevolge het constitutionele stelsel van de federatie, niet verplicht zijn wetgevende maatregelen te nemen, brengt de centrale regering de bevoegde autoriteiten van deze staten op de hoogte van de genoemde bepalingen, vergezeld van een gunstig advies, hen aanmoedigende om passende maatregelen te nemen ter effectuering hiervan.

Artikel 18

– Territoriale toepasselijkheid

1. Dit protocol is van toepassing op het grondgebied of de grondgebieden vermeld in een verklaring van een partij uit hoofde van artikel 38, lid 1 of lid 2, van het verdrag, voor zover die verklaring niet is ingetrokken uit hoofde van artikel 38, lid 3.

2. Een partij kan bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring verklaren dat dit protocol niet van toepassing is op een of meer in de verklaring van de partij uit hoofde van artikel 38, lid 1 en/of lid 2, van het verdrag vermelde grondgebieden.

3. Iedere uit hoofde van lid 2 van dit artikel afgelegde verklaring kan met betrekking tot elk in die verklaring aangegeven grondgebied worden ingetrokken door een aan de secretaris- generaal van de Raad van Europa gerichte kennisgeving. De intrekking wordt van kracht op de eerste dag van de maand die volgt op het verstrijken van een tijdvak van drie maanden na de datum van ontvangst van die kennisgeving door de secretaris-generaal.

Artikel 19

– Voorbehouden en verklaringen

1. Door middel van een schriftelijke kennisgeving aan de secretaris-generaal van de Raad van Europa kan iedere partij bij het verdrag, bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring, verklaren dat zij een of meer van de voorbehouden als bedoeld in artikel 7, lid 9, punten a) en b), artikel 8, lid 13, en artikel 17 van dit protocol maakt. Andere voorbehouden zijn niet toegestaan.

2. Door middel van een schriftelijke kennisgeving aan de secretaris-generaal van de Raad van Europa kan iedere partij bij het verdrag, bij de ondertekening van dit protocol of bij de nederlegging van haar akte van ratificatie, aanvaarding of goedkeuring, een of meer van de verklaringen afleggen als bedoeld in artikel 7, lid 2, punt b), en lid 8, artikel 8, lid 11, artikel 9, lid 1, punt b), en lid 5, artikel 10, lid 9, artikel 12, lid 3, en artikel 18, lid 2, van dit protocol.

3. Door elke partij bij het verdrag worden de verklaringen, kennisgevingen of mededelingen als bedoeld in artikel 7, lid 5, punten a) en e), artikel 8, lid 4, en lid 10, punten a) en b), artikel 14, lid 7, punt c), en lid 10, punt b), en artikel 17, lid 2, van dit protocol, overeenkomstig de daarin bepaalde voorwaarden, afgelegd door middel van een schriftelijke kennisgeving aan de secretaris-generaal van de Raad van Europa.

Artikel 20

– Status en intrekking van voorbehouden

1. Een partij die overeenkomstig artikel 19. lid 1, een voorbehoud heeft gemaakt, trekt dit voorbehoud geheel of ten dele in zodra de omstandigheden dit toelaten. Deze intrekking wordt van kracht op de datum van ontvangst van een aan de secretaris-generaal van de Raad van Europa gerichte kennisgeving. Indien in de kennisgeving wordt vermeld dat de intrekking van een voorbehoud van kracht moet worden op een daarin nader aangeduide datum, en deze datum later valt dan de datum waarop de kennisgeving door de secretaris-generaal wordt ontvangen, wordt de intrekking op deze latere datum van kracht.

2. De secretaris-generaal van de Raad van Europa kan met regelmatige tussenpozen bij de partijen die een of meer voorbehouden overeenkomstig artikel 19, lid 1, hebben gemaakt, informeren naar het mogelijke vooruitzicht op intrekking daarvan.

Artikel 21

– Wijzigingen

1. Wijzigingen van dit protocol kunnen worden voorgesteld door iedere partij bij dit protocol en worden door de secretaris-generaal van de Raad van Europa meegedeeld aan de lidstaten van de Raad van Europa, aan de partijen bij en ondertekenaars van het verdrag, alsmede aan iedere staat die uitgenodigd is toe te treden tot het verdrag.

2. Iedere door een partij voorgestelde wijziging wordt meegedeeld aan het Europees comité voor strafrechtelijke vraagstukken (CDPC), dat zijn advies over de voorgestelde wijziging voorlegt aan het Comité van Ministers.

3. Het Comité van Ministers onderzoekt de voorgestelde wijziging en het door het CDPC voorgelegde advies en kan, na raadpleging van de partij bij het verdrag, de wijziging aannemen.

4. De tekst van elke door het Comité van Ministers overeenkomstig lid 3 goedgekeurde wijziging wordt aan de partijen bij dit protocol ter aanvaarding toegezonden.

5. Iedere overeenkomstig lid 3 aangenomen wijziging treedt in werking dertig dagen nadat alle partijen de secretaris-generaal hebben meegedeeld dat zij de wijziging hebben aanvaard.

Artikel 22

– Beslechting van geschillen

Artikel 45 van het verdrag is van toepassing op dit protocol.

Artikel 23

– Beraadslagingen tussen de partijen en beoordeling van de tenuitvoerlegging

1. Artikel 46 van het verdrag is van toepassing op dit protocol.

2. De partijen beoordelen periodiek het feitelijke gebruik en de feitelijke uitvoering van de bepalingen van dit protocol. Artikel 2 van het reglement van orde van het comité Cybercrimeverdrag, zoals herzien op 16 oktober 2020, is van overeenkomstige toepassing. De partijen evalueren aanvankelijk de procedures van dat artikel zoals die van toepassing zijn op dit protocol en kunnen deze bij consensus wijzigen vijf jaar nadat dit protocol in werking is getreden.

3. De evaluatie van artikel 14 vangt aan zodra tien partijen bij het verdrag hebben verklaard ermee in te stemmen door dit protocol gebonden te zijn.

Artikel 24

– Opzegging

1. Iedere partij kan dit protocol te allen tijde opzeggen door middel van een kennisgeving aan de secretaris-generaal van de Raad van Europa.

2. De opzegging wordt van kracht op de eerste dag van de maand na het verstrijken van een tijdvak van drie maanden na de datum van ontvangst van de kennisgeving door de secretaris-generaal.

3. Opzegging van het verdrag door een partij bij dit protocol houdt opzegging van dit protocol in.

4. Informatie die of bewijsmateriaal dat is doorgegeven voorafgaand aan de datum waarop de opzegging van kracht wordt, wordt ook nadien overeenkomstig dit protocol behandeld.

Artikel 25

– Kennisgeving

De secretaris-generaal van de Raad van Europa stelt de lidstaten van de Raad van Europa, de partijen bij en ondertekenaars van het verdrag en iedere staat die is uitgenodigd om tot het verdrag toe te treden, in kennis van:
a. iedere ondertekening;
b. iedere nederlegging van een akte van ratificatie, aanvaarding of goedkeuring;
c. iedere datum van inwerkingtreding van dit protocol in overeenstemming met artikelen 16, leden 3 en 4;
d. iedere verklaring die is afgelegd en ieder voorbehoud dat is gemaakt overeenkomstig artikel 19 en iedere intrekking van een voorbehoud overeenkomstig artikel 20;
e. iedere andere handeling, kennisgeving of mededeling met betrekking tot dit protocol.

TEN BLIJKE WAARVAN de ondergetekenden, hiertoe naar behoren gemachtigd, dit protocol hebben ondertekend.

GEDAAN te Straatsburg op 12 mei 2022 in de Engelse en de Franse taal, zijnde beide teksten gelijkelijk authentiek, in één exemplaar dat zal worden neergelegd in het archief van de Raad van Europa. De secretaris-generaal van de Raad van Europa doet een gewaarmerkt afschrift toekomen aan iedere lidstaat van de Raad van Europa, aan iedere partij bij en iedere ondertekenaar van het verdrag en aan iedere staat die is uitgenodigd om tot het verdrag toe te treden.

D. PARLEMENT

Het Protocol behoeft ingevolge artikel 91 van de Grondwet de goedkeuring van de Staten-Generaal, alvorens het Koninkrijk aan het Protocol kan worden gebonden.

G. INWERKINGTREDING

De bepalingen van het Protocol zullen ingevolge artikel 16, derde lid, van het Protocol in werking treden op de eerste dag van de maand die volgt op het verstrijken van een tijdvak van drie maanden na de datum

waarop vijf staten bij het Verdrag, overeenkomstig de bepalingen van artikel 16, eerste en tweede lid, van het Protocol, hun instemming door het Protocol te worden gebonden tot uitdrukking hebben gebracht.

Uitgegeven de *vijfde* augustus 2022.

De Minister van Buitenlandse Zaken,

W.B. HOEKSTRA

trb-2022-66
ISSN 0920 - 2218
's-Gravenhage 2022