COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Strasbourg, 28 May 2021 T-CY (2021)12

Cybercrime Convention Committee (T-CY)

Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime

Summary of comments on opinions by Council of Europe Committees and submissions by other stakeholders on the draft 2nd Additional Protocol to the Convention on Cybercrime (May 2021)

Note prepared by T-CY Secretariat

Contents

Contact

Alexander Seger
Executive Secretary of the Cybercrime Convention Committee (T-CY)
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France
Email: alexander.seger@coe.int

1 Introduction

On 12 April 2021, the Protocol Drafting Plenary of the Cybercrime Convention Committee (T-CY) decided to publish a complete operative text and preliminary Explanatory Report of the draft 2nd Additional Protocol to the Budapest Convention on Cybercrime for consultations with relevant Council of Europe committees as well as civil society, data protection and industry stakeholders.

The online meeting, held on 6 May 2021, completed the sixth round of stakeholder consultations on this Protocol since July 2018. With respect to this last consultation round, written submissions have been received from Access Now, ADC, Canada Privacy Commission, CCBE, CENTR, CS Coalition, EuroISPA, EDPB, FRA, ICANN, Kaspersky, MARQUES, and New Zealand Privacy Commissioner.

In addition, written opinions have been received from the Council of Europe's European Committee on Crime Problems (CDPC) and the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD).

The purpose of the present summary is to provide informal comments to some of the issues raised by stakeholders.[1] Given the large number of points raised in the submissions and in the meeting on 6 May, it is not possible to provide detailed responses to all of them in this summary.

2 General comment on submissions received

- The contributions received during the previous five rounds of consultations since 2018 helped shape the Protocol as it evolved. As a result, some tools were not included in the Protocol and the system of safeguards was reinforced. The Protocol now also contains a detailed article on the protection of personal data.

- Experts from Parties to the Convention on Cybercrime from all regions of the world participated in the negotiations. A large number of meetings were held to prepare this Protocol, most of which were dedicated to safeguards. This included over sixty online meetings since the onset of the COVID-19 pandemic. Delegations participating in these meetings included data protection experts.

- The purpose of this Protocol is to provide tools in order to investigate crimes and obtain justice for victims. Given the prevalence of cybercrime in today's world, and the comparatively low number of criminal sanctions for cybercrime, it is important to provide victims of crime online an increased expectation of justice.

- The Protocol is a criminal justice treaty that applies to specific criminal investigations or proceedings related to cybercrime and evidence on computer systems (see Article 2 – Scope of application). It is not an instrument for national security purposes, nor does it provide for mass surveillance or bulk collection of data. It is also not a treaty to establish or harmonise comprehensive data protection regimes.

[1] Note: These informal comments are provided in recognition of the contributions made by stakeholders. However, they do not necessarily reflect the views of the drafters of the Protocol; those are reflected in the Explanatory Report to the Protocol.

- This is an additional Protocol (not an amending one) and a State can only become a Party after joining the Convention and subscribing to its standards, including its safeguards (Article 15), first.

- Neither the Budapest Convention nor the Protocol contain provisions requiring indiscriminate data retention by providers for a defined period of time. Rather, the Convention contains measures that apply to preservation of specified data needed in the context of a specific criminal investigation or proceeding.

- The tools of the Protocol will not be applied by Parties in isolation but will need to be implemented and embedded in the domestic legal framework of a Party. The criminal justice systems of Parties include safeguards and mechanisms for supervision.

- The Budapest Convention is a treaty with currently 66 Parties (including 21 that are not member States of the COE and 40 that are not members of the European Union). The Protocol needs to work for all of them and other countries that seek to become Parties. Provisions need to be clear and sufficiently specific and detailed on the one hand, but at the same time leave a sufficient level of flexibility to permit adaptation to different legal systems and to evolving technology, business models and interpretation by courts.

- While the Parties to the Convention have created a mechanism through the T-CY to carry out assessments of implementation of the Convention, under this Protocol such assessments will become a treaty requirement under Article 23.

3 Opinions by Council of Europe committees

3.1 European Committee on Crime Problems (CDPC)

3.1.1 Summary of points raised by the CDPC

Following a request by the T-CY Secretariat, on 5 May 2021 the European Committee on Crime Problems (CDPC) submitted an opinion on the draft 2nd Additional Protocol that had been prepared by the PC-OC[2] and endorsed by the CDPC.

Overall, the CDPC is supportive of the draft Protocol and considers that it "will bring a real added value to international cooperation in the area of cybercrime and the obtention of evidence in electronic form".

The CDPC/PC-OC would have preferred:

- while welcoming the provisions on cooperation in emergencies, clarification of the concept of "safety of a person" in the definition of "emergency";

- closer alignment of Article 11 (video conferencing) with the corresponding provision of the 2nd Additional Protocol to the Convention on Mutual Assistance in Criminal Matters (ETS 182) but acknowledges that, with regard to videoconferences, the Protocol would not apply to Parties to ETS 182.

[2] Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (subordinate body of the CDPC).

3.1.2 Comment

- In defining the term "emergency", the draft Protocol provides a margin of flexibility to Parties as to how to apply it regarding the safety of a natural person; examples are provided in the Explanatory Report of such situations (see paragraphs 41-42 of the Explanatory Report).

- The T-CY Protocol Drafting Group benefitted from previous exchanges with members of the PC-OC and therefore has clarified the relationship between provisions of this Protocol and other relevant treaties, in particular ETS 182, in the operative text (see Article 5) and the Explanatory Report(see, for example, paragraphs 62-67, 69, 182-186).

3.2 Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD)

3.2.1 Summary of points raised by the T-PD

In response to a request from the T-CY Secretariat, on 7 May 2021 the T-PD provided an opinion on the draft 2nd Additional Protocol.

The T-PD acknowledged that Article 14 of the draft Protocol on the protection of personal data is a compromise reached in negotiations with a wide range of countries and legal systems, recognised the potential of such stand-alone provisions and welcomes that its implementation will be assessed under Article 23. It furthermore recognises that Article 14 is not aimed at harmonising national data protection regimes. In this context, the T-PD invites Parties to the Budapest Convention and its future Protocol to accede to Convention 108+ in view of greater convergence of rules for the protection of personal data.

The T-PD makes a number of suggestions regarding Article 14:

- To further underline the standards of paragraphs 2-15 when Parties choose options 1.b or 1.c for the transfer of personal data;

- To confirm in the Explanatory Report that Convention 108+ qualifies per se as an agreement referred to in paragraph 1.b;

- To avoid that under option 1.c personal data are transferred without any data protection safeguards;

- To further clarify in paragraph 4 the term "considered sensitive in view of the risks involved";

- To extend paragraph 8 (maintaining records) to include "storage" and "use";

- To require that for international onward transfers (paragraph 10), the transferring authority give due regard to an appropriate level of protection in line with Article 14.

Regarding Articles 7 and 8, the T-PD proposes that the Protocol clarify "when a service provider is considered 'physically present' in a Party's territory".

Regarding Article 8, the T-PD proposes to apply for the disclosure of traffic data the combined data protection and other safeguards of the requesting Party, of the Party where the data subject was present whilst using the targeted service, and of the Party of the location of the service provider.

Regarding Articles 6 and 7, the T-PD proposes "hard confidentiality" requirements for providers as foreseen for Article 9.

3.2.2 Comment

- Option 1.b under Article 14 only applies to international agreements establishing a comprehensive framework for the protection of personal data, applicable to the transfer of personal data for the purpose of prevention, detection, investigation and prosecution of criminal offences, *and* that provide that the processing of personal data under that agreement complies with the requirements of the data protection legislation of the Parties concerned. Therefore, as a practical matter, the provisions of such agreements (for many Parties this is likely to be Convention 108+) are likely to be similarly or even more comprehensive and specific than those of Article 14, paragraphs 2 to 15.

- Explanatory Report paragraph 224 makes specific reference to Convention 108+ as an agreement applicable under option 1.b. The terms of Convention 108+ would apply as between Parties to that convention, with respect to measures falling within the scope of such agreement, to personal data received under the Protocol in lieu of paragraphs 2 to 15 of Article 14.

- Option 1.c would apply only between Parties whose agreements or arrangements permit the application of different standards; in this regard, some delegations have referred to existing mutual assistance agreements.

- Article 14, paragraph 4, covers "sensitive data". Paragraph 237 of the Explanatory Report explains that "while certain forms of biometric data may be considered sensitive in view of the risks involved, other forms may not." Because the level of sensitivity of biometric data may vary, Parties are granted some flexibility how to regulate this area. Some of the concepts used in Convention 108+ (including the term "resulting from a specific technical processing" in paragraph 58 of the Explanatory Report to Convention 108+) may also be understood differently in different parties to the Convention on Cybercrime. Following the opinion of the T-PD, the following clarification was added to paragraph 237 of the Explanatory Report to the Protocol: "With respect to the Parties to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), as amended by Protocol (CETS No. 223), the interpretation of what constitutes "sensitive" biometric data should be guided by Article 6, paragraph 1, of that Convention, as further detailed in paragraphs 58 and 59 of that Convention's Explanatory Report."

- Article 14, paragraph 8, includes "used" and "accessed"; the added value of adding "stored" is unclear.

- With regard to Article 14, paragraph 10, Explanatory Report paragraph 265 addresses the point made by T-PD.

- The understanding of when a service provider is considered "physically present" may vary among legal systems, and may also be evolving; despite such limitations, the drafters provided clarification in paragraphs 99 and 128 of the Explanatory Report.

- The feasibility of applying the combined data protection safeguards of potentially the requesting Party, the Party of the service provider and of the Party where the data subject was present when using the targeted service without unreasonable effort is unclear as the identity and location of a person is generally not known at the outset of an investigation. It may also require additional investigations to identify the place of residence of a user. Finally, such an approach increases burdens beyond what is even required under mutual assistance regimes.

- The direct cooperation provisions provide a basis for requesting Parties to provide special procedural instructions in order to seek confidentiality to the extent possible, for example, subject to requirements under domestic law. In some Parties, confidentiality of the request will be maintained by operation of law, while in other Parties this is not necessarily the case (see paragraphs 84.d and 106 of the Explanatory Report).

4 Submissions by other stakeholders

4.1 Comments on submissions related to Chapter II (Measures for enhanced cooperation)

4.1.1 The Protocol should not lower standards

- Concerns that the Protocol is lowering standards and protections are not justified. As any multilateral treaty, this Protocol needs to take into account that Parties have different legal systems and thus also different systems of protections. The Protocol foresees reservations, declarations and other provisions to take into account standards and protections of Parties and ensure that they are not lowered (examples are the declarations in Article 7, paragraph 2.b, and in Article 7, paragraph 5).

- The Protocol creates a clear framework with safeguards. Moreover, unlike other international instruments on cooperation in criminal matters, the Protocol includes a very detailed article on the protection of personal data transferred under this Protocol.

4.1.2 Mutual assistance should be favoured over direct requests or orders

- Mutual legal assistance (MLA) is, and is likely to remain, the main means to obtain a wide range of evidence from other jurisdictions for use in criminal proceedings. The T-CY, following detailed analyses, in 2014 agreed on a set of recommendations to render MLA related to cybercrime and electronic evidence more efficient. Follow-up was given to these recommendations by Parties to the Budapest Convention, the T-CY and through capacity building projects; and MLA-type measures were also included in this Protocol (Articles 10, 11 and 12).

- However, the T-CY also concluded that for some type of information or in some circumstances, other ways of cooperation need to be made available. This is particularly true for subscriber information and domain name registration information. If requests or orders for such information can be handled through direct cooperation, the MLA systems

would have more resources available for more complex requests and cases requiring more intrusive measures.

4.1.3 Mandatory judicial or other independent approval of requests or orders

- Parties to the Budapest Convention have different requirements for obtaining different types of data. Depending on their domestic legal system, evidence may be sought or authorised by prosecutors, grand juries, investigating magistrates, judges or other authorities. Given different regimes in Parties, it was considered disproportionate to require judicial authorisation in all cases. In order to accommodate the need of some Parties to have an additional safeguard of further review of the legality of the order, Article 7, paragraph 2.b permits Parties to make a declaration stating that "the order under paragraph 1 must be issued by, or under the supervision of, a prosecutor other judicial authority, or otherwise be issued under independent supervision" (see also paragraph 101 of the Explanatory Report to the Protocol).

- It was considered disproportionate to require judicial authorisation with regard to requests for domain name registration information under Article 6, as the provision (in paragraph 1) only provides a basis for requests and (in paragraph 2) requires Parties to ensure that such entities are permitted to disclose the requested data. In addition, registration data comprises basic information that may be considered only a limited subset of subscriber data and does not permit precise conclusions to be drawn concerning the private lives and daily habits of individuals (see paragraphs 80 and 82 of the Explanatory Report). In Furthermore, requests are limited to specific criminal investigations or proceedings; disclosure is subject to reasonable conditions provided by domestic law; and the safeguards of Articles 13 and 14 apply.

- Not all legal systems require ex-ante judicial review with respect to measures provided in this Protocol but allow for subsequent judicial involvement in proceedings. Mandating a singular model would not be feasible given the large number of Parties to the Convention.

4.1.4 Mandatory notification to the authorities or requested States or States of residence

- While some Parties saw the need for being notified if another Party sends an order for subscriber information to a provider in their territory under Article 7 in any or specified circumstances, others were concerned that their central authorities might be overwhelmed by large numbers of notifications, or that it may not be necessary in all situations. In order to address such requirements and concerns, Parties were provided with the ability to require notification pursuant to Article 7, paragraph 5.

- As indicated above in relation to comments by the T-PD, notification of the State of residence poses a number of challenges for States (possibly in addition to the State of the service provider) and would create a disproportionate burden for investigating authorities as it may require an additional investigation to determine the place of residence and add a requirement that would normally not have to be met for mutual assistance.

4.1.5 Mandatory notification to the person whose data is sought

- The domestic laws of Parties vary in terms of if and when subjects may or must be notified in a criminal investigation. The question of notification, and of limitations to such notification, is addressed in paragraph 11 of Article 14.

4.1.6 Allowing private sector entities to consult with authorities regarding a request and/or to object to it

- Articles 6 and 7 are designed in a way to avoid back and forth exchanges by specifying what information must be provided in requests and orders. Under Article 7, paragraph 5.b, a Party may require a service provider in its territory to consult its authorities in identified circumstances (see also paragraph 108 of the Explanatory Report).

4.1.7 Creation of public oversight mechanisms, transparency and statistics

- Proposals to the effect that cross-border requests, including for emergency disclosure (Article 9), must be subject to a public oversight mechanism, would not be compatible with rule of law principles to the extent that such oversight bodies would oversee the criminal justice system. Criminal justice authorities are closely regulated and subject to oversight at all stages. This is also true for joint investigation teams (Article 12), which are subject to oversight, and coercive actions in each participating Party may require judicial authorisation.

- The collation of annual statistics on requests to service providers may be one of the tasks of the T-CY when following up on the implementation of the Protocol by the Parties. In fact, the T-CY in its preparatory work for the Protocol (T-CY Cloud Evidence Group) had made ample use of data published by service providers in their transparency reports. However, there was no intent to require service providers to issue such reports. As follow-up to the consultations, paragraph 106 of the Explanatory Report was revised to clarify that a "request for confidentiality should not prevent service providers from transparency reporting on anonymised aggregate numbers of orders received under this Article."

4.1.8 Article 6 (requests for domain name registration information)

- Regarding the question as to whether Article 6 applies to entities providing domain name registration services or any "entities providing domain name services", including domain name resolution services, resellers or privacy proxy providers, the former is the case (see Article 6, paragraph 1, which now refers to "a request to an entity providing domain name registration services").

- Regarding the proposal to require that, under Article 6, paragraph 2, the permission of an entity to disclose information be "subject to reasonable and proportionate conditions provided by domestic law, including a clear legal basis", paragraph 2 provides that disclosure may be "subject to reasonable conditions provided by domestic law", and paragraph 82 of the Explanatory Report specifies that "in some Parties [this] may include data protection conditions".

- Article 6 is subject to Articles 13 and 14 of the Protocol.

- A requirement to notify the State of the entity simultaneously when requests are sent was considered unnecessary considering the nature of that information and the fact that this provision is anticipated to be complementary to relevant internet governance multi-stakeholder policies (paragraph 76 of the Explanatory Report). Requiring notification would contradict such policies and practices.

- Article 6 is a measure specific to domain name registration information and is less complex than Article 7. Depending on the circumstances and domestic law, an entity providing domain name registration services may also be considered a service provider and domain name registration information may also be considered (a subset) of subscriber information and thus it is not excluded that in such situations Article 7 is used to obtain the disclosure of domain name registration information.

4.1.9 Article 7 (disclosure of subscriber information)

- Regarding the proposal to clarify the term "subscriber information" and to exclude traffic data, paragraphs 92 and 93 of the Explanatory Report already provide such clarification. Moreover, Parties may make a reservation under Article 7, paragraph 9.b, not to apply this Article to certain types of access numbers if this would be inconsistent with fundamental principles of their domestic legal systems.

- Regarding respect for legal professional privilege and similar privileges, this provision permits Parties that elect to be notified to invoke grounds for refusal in applicable mutual assistance treaties or domestic laws, which provides "safeguards for the rights of persons located in the requested Party" (clarification added to Explanatory Report paragraph 141 following the consultations). In any event, Article 7 only pertains to subscriber information and not, for example, to privileged communications between attorneys and their clients.

- Regarding the proposal to develop templates for requests to service providers, this may be taken up by the T-CY (as done previously for the Convention) to facilitate cooperation, as was previously done for preservation and mutual assistance requests.

4.1.10 Article 12 (joint investigation teams and joint investigations)

- When measures are carried out in a Party participating in a JIT, the authorities of that Party determine whether they can take the investigative measure on the basis of their domestic law.

- As also explained above, JITs are subject to the oversight mechanisms of the criminal justice system.

- Publication of the terms of a JIT agreement may violate regulations regarding the secrecy of investigations or even the rights of persons under investigation.

4.2 Comments on submissions related to Chapter III (Safeguards)

4.2.1 General comment

- The measures of the Protocol are subject to multiple safeguards in addition to Articles 13 and 14, for example:

  - the measures of the Protocol apply only to specific criminal investigations and proceedings;
  - Parties need to "adopt such legislative and other measures as may be necessary to carry out the obligations set forth in this Protocol" in their domestic law (see the general rule in Article 2, paragraph 2; and its iterations, for example, in Article 6, paragraph 2, or Article 7, paragraph 2);
  - articles list what orders or requests shall specify and what supplemental information shall be provided (see for example Article 7, paragraphs 3 and 4);
  - reservations and declarations permit Parties to meet specific requirements of their domestic law (for example, the notification regime of Article 7, paragraph 5); and
  - use limitations, confidentiality requirements or grounds for refusal may apply.

- And importantly, the measures of the Protocol will be embedded in the criminal justice system of a Party and each Party is required to ensure that the establishment, implementation and application of the powers provided for in this Protocol are subject to conditions and safeguards provided under its domestic law, which shall provide for the adequate protection of human rights and liberties (Article 13; see also Article 15 to the Convention).

- Regarding the proposal to make the measures of the Protocol available to obtain information or evidence for the purpose of the defence of an accused (which some commentators referred to as "equality of arms"), this issue is not regulated in the Convention on Cybercrime. Rather, it is subject to the domestic law of a Party and therefore it would not be possible to establish a general rule for this in this Protocol.

4.2.2 Article 13 (conditions and safeguards)

- Article 13 adapts Article 15 of the Convention to the measures of the Protocol. Article 13 provides that, "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 15 of the Convention provides that "Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties … and which shall incorporate the principle of proportionality." Like Explanatory Report paragraph 146 to the Convention, Explanatory Report paragraph 218 to this Protocol provides that "the principle of proportionality 'shall be implemented by each Party in accordance with relevant principles of its domestic law'".

4.2.3 Article 14 (protection of personal data)

Note: At the time of the consultations, the Explanatory Report to the Protocol regarding Article 14 was not yet available. In the meantime, a number of proposals made and questions raised by stakeholders have been addressed in the Explanatory Report.

- A large number of Parties to the Budapest Convention are also Parties to data protection Convention 108 of the Council of Europe, and the Council of Europe has been supporting countries in the reform of data protection regulations in line with Convention 108 to facilitate accession to that convention. Convention 108+ is not yet in force, but the Council of Europe is following a similar approach for it. However, it is not possible to make accession to Convention 108 or Convention 108+ a requirement for becoming a Party to the Budapest Convention or its Protocols. Article 14, in paragraph 1.b, provides that, as between parties to that convention, the terms of that convention apply, for the measures falling within the scope of such agreement, to personal data received under the Protocol in lieu of paragraphs 2 to 15 of Article 14.

- The Protocol, in its Article 14, provides for core data protection requirements ranging, for example, from "purpose and use", "quality and integrity", "maintaining records" and "data security and security incidents" to "access and rectification" and "judicial and non-judicial redress".

- Article 14 also requires "independent and effective oversight" pursuant to the terms of paragraph 14. However, it would not be compatible with rule of law principles if such oversight bodies had the competency to oversee the criminal justice system, for example, by controlling orders or requests as suggested by some.

- Regarding the suggestion that Parties may unilaterally impose at any time any additional data protection requirements, this would defeat the purpose of Article 14 to provide a basis for international transfers of personal data by ensuring appropriate safeguards. As explained in paragraph 224 of the Explanatory Report, paragraph 1.d of Article 14 "provides legal certainty for international transfers of personal data in accordance with paragraphs 1.a or 1.b in response to orders and requests under the Protocol in order to ensure the effective and predictable exchange of data". And paragraph 225 of the Explanatory Report explains that in addition, "paragraph 1.d provides that a Party may only refuse or prevent personal data transfers to another Party under this Protocol for reasons of data protection: (i) under the conditions set out in paragraph 15 regarding consultations and suspensions, when paragraph 1.a applies, or (ii) under the terms of the specific agreements or arrangements referred to in paragraphs 1.b or 1.c, when one of those paragraphs applies."

- Regarding the processing of data for a "legitimate purpose", Article 14, paragraph 2 (purpose and use), makes it clear that the "Party that has received personal data shall process such data for the purposes described in Article 2" of the Protocol. Article 2 defines the "scope of application" of the Protocol, namely, that it applies to "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" (see also paragraphs 227 to 231 of the Explanatory Report). The Explanatory Report 227 further explains, "authorities must be investigating or prosecuting specific criminal activity, which is the legitimate purpose for which evidence or information containing personal data may be obtained and processed."

- It is recalled that "[e]ach Party shall adopt such legislative and other measures as may be necessary to carry out the obligations set forth in this Protocol" (see Article 2, paragraph 2; see also Article 6, paragraph 2, Article 7, paragraph 2).

- "Retention periods" are covered by Article 14, paragraph 5, and further explained in paragraphs 240 to 242 of the Explanatory Report. "Record keeping" is covered by Article 14, paragraph 8, and further explained in paragraphs 257 to 258 of the Explanatory Report. Criminal justice systems typically have detailed rules for retention periods, but such periods may differ between Parties. A margin of discretion as to how Parties regulate these in detail must therefore be granted.

- Regarding the suggestion concerning Article 14, paragraph 11.a, that the reference to how general notices are handled lacks implementation details and that this could be addressed by referencing an "organizational website or other publicly accessible media", this has been taken into account and made clear in Paragraph 267 of the Explanatory Report.

- Regarding the proposal to include in Article 12 that individuals receive confirmation of processing, an additional explanation was inserted into paragraph 271 of the Explanatory Report, that this "may also allow the individual to confirm whether (or not) their personal data has been obtained under the Protocol, and has been or is being processed" (clarification added following the consultations).

- Regarding restrictions to the entitlement to access under Article 14, paragraph 12, paragraph 272 of the Explanatory Report now also clarifies that "proportionate restrictions must protect the rights and freedoms of others or protect important objectives of general public interest and give due regard to the "legitimate interests of the individual concerned". The phrase "legitimate interests of the individual concerned" was considered by the drafters to include the individual's rights and freedoms".

- Regarding proposals related to "oversight" (paragraph 14 of Article 14), the operative text was amended to include "the power to act upon complaints", and paragraph 281 of the Explanatory Report was amended to include that "Consultations between the Parties' respective authorities when carrying out their oversight functions under this Article may take place as appropriate".

- Regarding the suggestion that in situations of onward sharing (Article 14, paragraph 9) the transferring authority should be informed of the envisioned onward sharing and further processing, the Parties considered that the added-value of such information is not apparent, in view of the safeguards already included in the Protocol, in particular in Article 14 on data protection.

- Regarding the involvement of data protection experts in the assessments pursuant to Article 23 of the Protocol, an additional sentence was added to paragraph 322 of the Explanatory Report stating that in "view of the relevant expertise necessary for the assessment of the use and implementation of some of the provisions of this Protocol, including on Article 14 on data protection, Parties may consider involving their subject-matter experts in the assessments." This may include, for instance, representatives of data protection authorities.

5 Conclusion

This sixth round of consultations – as the previous ones – helped shape the draft Protocol. Following the meeting of 6 May 2021 and a review of the written submissions, a number of changes were introduced to the draft of the Protocol.

With regard to other proposals and queries, the informal comments of this summary are provided in recognition of the contributions, queries, and proposals made by stakeholders. However, as stated above, they do not necessarily reflect the views of the drafters of the Protocol; those are reflected in the Explanatory Report to the Protocol.

This Protocol is a complex instrument and the result of detailed negotiations among a large number of countries with diverse legal systems. More than ninety meetings over almost four years were necessary to achieve an outcome in the form of this draft Protocol that reconciles measures for an effective criminal justice response with strong rule of law and data protection safeguards.

6 Appendix

6.1 Agenda of the consultations on 6 May 2021

Cybercrime Convention Committee (T-CY)

Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime

6th round of consultations with stakeholders

Virtual meeting, 12h00 – 18h00 (France), 6 May 2021

12h00-14h30	**Part 1: Overview and review of Chapter II**
	Opening remarks
	Overview of the draft Protocol
	Chapter II: Summary of written submissions[3]
	Discussion
14h30-16h00	Break
16h00-18h00	**Part 2: Safeguards**
	Overview of the safeguards of the Protocol
	Presentation of Article 14 on data protection
	Discussion

[3] Written submissions and the draft text of the Protocol are available at Protocol Consultations (coe.int)

6.2 List of participants

T-CY Cybercrime Convention Committee
Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime
6th round of consultations with stakeholders – 6 May 2021

COUNTRIES / *PAYS*

ARGENTINA / *ARGENTINE*	Dominique PAZ Cybercrime Prosecutor Office / *Bureau du procureur chargé de la cybercriminalité*
ARGENTINA / *ARGENTINE*	Aldana ROHR Ministry of Foreign Affairs / *Ministère des affaires étrangères*
ARGENTINA / *ARGENTINE*	Agustina SIRVEN AAIP / *AAIP*
ARGENTINA / *ARGENTINE*	Mauro MELONI Personal Data Protection National Agency / *Agence nationale de protection des données personnelles*
ARGENTINA / *ARGENTINE*	Eduardo CIMATO Personal Data Protection National Agency / *Agence nationale de protection des données personnelles*
ARGENTINA / *ARGENTINE*	Cecilia GARIBOTTI Personal Data Protection National Agency / *Agence nationale de protection des données personnelles*
AUSTRALIA / *AUSTRALIE*	Nathan WHITEMAN Department of Home Affairs / *Département des affaires intérieures*
AUSTRALIA / *AUSTRALIE*	Emily HITCHMAN Department of Home Affairs / *Département des affaires intérieure*
BELGIUM / *BELGIQUE*	Delphine WYNANTS Federal Public Service Justice / *Service Public Fédéral Justice*
CANADA / *CANADA*	Normand WONG Ministry of Justice / *Ministère de la Justice*
CANADA / *CANADA*	Tom BEVERIDGE Counsellor, International Criminal Operations Mission of Canada to the EU / *Conseiller, Mission d'opérations criminelles internationales du Canada auprès de l'UE*
CANADA / *CANADA*	Philip LUPUL Criminal, Security, Diplomatic Law Division / *Division du droit pénal, de la sécurité et du droit diplomatique*
CANADA / *CANADA*	Gareth SANSOM Federal Department of Justice / *Département fédéral de la justice*
CANADA / *CANADA*	Jacqueline PALUMBO Ministry of Justice / *Ministère de la Justice*
CANADA / *CANADA*	Anne-Marie LE BEL Ministry of Justice / *Ministère de la Justice*
CANADA / *CANADA*	Tebello MOROJELE Global Affairs / *Affaires mondiales*

CANADA / *CANADA*	Ian DOUGLAS Office of the Privacy Commissioner of Canada / *Commissariat à la protection de la vie privée du Canada*
COLOMBIA / *COLOMBIE*	Jefferson Rolando ROJAS RODRIGUEZ Attorney's General Office / *Bureau du procureur général*
COLOMBIA / *COLOMBIE*	Juan Pablo SALAZAR HOYOS Ministry of Information and Communication Tehcnologies / *Ministère des technologies de l'information et de la communication*
COLOMBIA / *COLOMBIE*	Diana Carolina KECAN CERVANTES Ministry of Foreign Affairs / *Ministère des affaires étrangères*
COLOMBIA / *COLOMBIE*	Jehudi CASTRO Presidency of the Republic / *Présidence de la République*
CROATIA / *CROATIE*	Zrinka SALAJ Ministry of Foreign Affairs / *Ministère des affaires étrangères* Permanent Representation of Croatia to the European Union / *Représentation permanente de la Croatie auprès de l'Union européenne*
CZECH REPUBLIC / *RÉPUBLIQUE TCHÈQUE*	Jakub PASTUSZEK Ministry of Justice / *Ministère de la Justice*
DOMINICAN REPUBLIC / *RÉPUBLIQUE DOMINICAINE*	Cesar MOLINE RODRIGUEZ Institute for Telecommunications */ Institut des télécommunications*
ESTONIA / *ESTONIE*	Markko KÜNNAPU Ministry of Justice / *Ministère de la Justice*
FINLAND / *FINLANDE*	Janne KANERVA Ministry of Justice / *Ministère de la Justice*
FRANCE / *FRANCE*	Caroline BOTSCHI Ministry of Justice / *Ministère de la Justice*
FRANCE / *FRANCE*	Etienne MAURY CNIL / *Conseiller juridique et CNIL*
GERMANY / *ALLEMAGNE*	Sara CLAASSEN Federal Ministry of Justice and Consumer Protection / *Ministère fédéral de la justice et de la protection des consommateurs*
GERMANY / *ALLEMAGNE*	Lisa BÜTTGEN German DPA (BfDI, Federal Commissioner for Data Protection and Freedom of Information) / Autorité allemande de protection des données (BfDI, Commissaire fédéral à la protection des données et à la liberté d'information)
GERMANY / *ALLEMAGNE*	Frederic BARTH Federal Ministry of Justice and Consumer Protection / *Ministère fédéral de la justice et de la protection des consommateurs*
JAPAN / *JAPON*	Satoshi YANAGISAWA Ministry of Foreign Affairs/ *Ministère des affaires étrangères*
JAPAN / *JAPON*	Hideaki KOJIMA Consulate General of Japan in Strasbourg / *Consulat général du Japon à Strasbourg*
JAPAN / *JAPON*	Kazunori SONOHARA National Police Agency / *Agence nationale de la police*

LATVIA / *LETTONIE*	Kristina TIMOFEJEVA National Police / *Police nationale*
LATVIA / *LETTONIE*	Olegs OLINS State Police of Latvia / *Police d'État de Lettonie*
NORWAY / *NORVÈGE*	Eirik Trønnes HANSEN Prosecutor / *Procureur*
NORWAY / *NORVÈGE*	Catharina LURÅS Ministry of Justice and Public Security / *Ministère de la Justice et de la sécurité publique*
PORTUGAL / *PORTUGAL*	Maria-José CASTELLO-BRANCO Ministry of Justice / *Ministère de la Justice*
PORTUGAL / *PORTUGAL*	Pedro VERDELHO T-CY Vice-Chair / *T-CY Vice-Président* Public Prosecutor / *Procureur général* General Prosecutor's Office of Lisbon / *Bureau du procureur général de Lisbonne*
REPUBLIC OF KOREA / *CORÉE DU SUD*	Min Goo Kim Korean National Police Agency / *Agence de la Police Nationale*
REPUBLIC OF KOREA / *CORÉE DU SUD*	Seung CHOI KSPO (Korean Supreme Prosecutor's Office) / *KSPO (Bureau du procureur suprême de Corée)*
REPUBLIC OF KOREA / *CORÉE DU SUD*	Representative / Représentant.e National Police / *Police nationale*
ROMANIA / *ROUMANIE*	Cristina SCHULMANN T-CY Chair / *T-CY Présidente* Department for International Law and Judicial Cooperation / *Département pour le droit international et la coopération judiciaire* Ministry of Justice / *Ministère de la Justice*
SERBIA / *SERBIE*	Branko STAMENKOVIC Public Prosecutor's Office / *Bureau du procureur*
SLOVAKIA / *SLOVAQUIE*	Branislav BOHACIK Republic Prosecutor's Office / *Bureau du procureur de la République*
SLOVAKIA / *SLOVAQUIE*	Zuzana ŠTOFOVÁ Ministry of Justice / *Ministère de la Justice*
SPAIN / *ESPAGNE*	Maria Elvira TEJADA DE LA FUENTE General Prosecutor's Office / *Bureau du procureur général*
SRI LANKA / *SRI LANKA*	Jayantha FERNANDO CERT / *CERT*
SRI LANKA / *SRI LANKA*	K.D.G.L Ashoka DHARMASENA Police / *Police*
SRI LANKA / *SRI LANKA*	B.V.I GAYASRI Police / *Police*
SRI LANKA / *SRI LANKA*	Ravindu MEEGASMULLA CERT / *CERT*

SRI LANKA / *SRI LANKA*	Buddhika WIJAYASUNDARA Police / *Police*
TURKEY / *TURQUIE*	Gökçen ÇEVİK Ministry of Justice / *Ministère de la Justice*
TURKEY / *TURQUIE*	Guray GÜÇLÜ Permanent Representation of Turkey to the CoE/ *Représentation permanente de la Turquie auprès du CoE*
UNITED KINGDOM / *ROYAUME UNI*	Representative / Représentant.e Home Office / *Ministère de l'Intérieur*
UNITED KINGDOM / *ROYAUME-UNI*	Priya MISTRY Home Office / *Ministère de l'Intérieur*
USA / *ÉTATS-UNIS D'AMÉRIQUE*	Benjamin FITZPATRICK Department of State / *Département d'État*
USA / *ÉTATS-UNIS D'AMÉRIQUE*	Kenneth HARRIS Senior Counsel for European Union and International Criminal Matters United States Mission to the European Union / *Conseiller principal pour les questions relatives à l'Union européenne et aux affaires pénales internationales, Mission des États-Unis auprès de l'Union européenne*
USA / *ÉTATS-UNIS D'AMÉRIQUE*	Sheri SHEPHERD-PRATT Department of Justice / *Département de la justice*
USA / *ÉTATS-UNIS D'AMÉRIQUE*	Katherine HARMAN-STOKES Department of Justice / *Département de la justice*
USA / *ÉTATS-UNIS D'AMÉRIQUE*	Erica O'NEIL Department of Justice / *Département de la justice*
USA / *ÉTATS-UNIS D'AMÉRIQUE*	Katie EINSPANIER Department of State / *Département d'État*
USA / *ÉTATS-UNIS D'AMÉRIQUE*	Hannah MAYER Department of Justice / *Département de la justice*
USA / *ÉTATS-UNIS D'AMÉRIQUE*	Benjamin FITZPATRICK Department of State / *Département d'État*

ORGANISATIONS

EDPS / *EDPS*	Representative / Représentant.e
European data protection supervisor	Niksa STOLIC Legal Officer / *Conseillère juridique*
EUROPEAN UNION AGENCY FOR CYBERSECURITY / *AGENCE EUROPÉENNE DE CYBER-SÉCURITÉ*	Silvia PORTESI Cybersecurity Expert / *Expert sécurité*
EUROPEAN UNION - EUROPEAN COMMISSION /	Tjabbe BOS DG HOME / *DG Home*

UNION EUROPEENNE, COMMISION EUROPEENNE	
EUROPEAN UNION - EUROPEAN COMMISSION / *UNION EUROPEENNE, COMMISION EUROPEENNE*	Manuel GARCIA SANCHEZ (DJ JUST) International data flows and protection / *(DJ JUST) Flux de données et protection au niveau international*
EUROPEAN UNION - EUROPEAN COMMISSION / *UNION EUROPEENNE, COMMISION EUROPEENNE*	Gemma CAROLILO Next-generation Internet / *Internet de nouvelle génération*
EUROPEAN UNION - EUROPEAN COMMISSION / *UNION EUROPEENNE, COMMISION EUROPEENNE*	Melnia STROUNGI Next-generation Internet / *Internet de nouvelle génération*
Council of the EU / *Conseil de l'Union européenne*	Leila BEZDROB Trainee / *Stagiaire*
Council of the EU / *Conseil de l'Union européenne*	Maria CASTILLEJO Political Administrator / *Administratrice politique*
Council of the EU / *Conseil de l'Union européenne*	Christina STROMHOLM Administrator / *Administratrice*

ACADEMIA, NON GOVERNMENTAL ORGANISATIONS AND PRIVATE SECTOR / *UNIVERSITES, ORGANISATIONS NON GOUVERNEMENTALES ET SECTEUR PRIVE*

Access Now	Estelle MASSE	Senior Policy Analyst / *Analyste politique principale*
Access Now	Raman Jit Singh CHIMA	Senior International Counsel and Global Cybersecurity Lead / *Avocat international senior et Responsable de la cybersécurité globale*
ADC	Alejo KIGUEL	Analyst / *Analyste*
APPLE	Representative / Représentant.e	Privacy Counsel / *Conseiller.e en protection de la vie privée*
Binalyze OU	Klaus Peter Finke Härkönen	Strategic Advisor / *Conseiller en stratégie*
CCIA	Alexandre ROURE	Senior Manager, Public Policy / *Directeur principal, politique publique*
CENTR,	Polina MALAJA	Policy Advisor / *Conseillère en politique*
Com Laude Group	Susan PAYNE	Head of Legal Policy / *Cheffe de la section politique juridique*
Com Laude Group	Sophie HEY	Policy Advisor / *Conseillère en matière de politique*

Council of Bars and Law Societies of Europe (CCBE)	Representative / Représentant.e	
Council of Bars and Law Societies of Europe (CCBE)	Martin SACLEUX	Legal advisor / *Conseiller juridique*
Council of Bars and Law Societies of Europe (CCBE)	Representative / Représentant.e	
Derechos digitales	Maria PAZ CANALES	Executive Director / *Directrice exécutive*
EHFCN	Dimitra LINGRI	Managing Director / *Directrice*
Electronic Frontier Foundation	Katitza RODRIGUEZ	Policy Director for Global Privacy / *Directrice de la politique de confidentialité mondiale*
EuroISPA	Andreas GRUBER	Chair of the Cybersecurity Committee / *Président du Comité sur la cybersécurité*
European Healthcare anti Fraud and Corruption Network	Dimitra LINGRI	Managing Director / *Directrice générale*
European Digital Rights	Chloé BERTHÉLÉMY	Policy Advisor / *Conseillère en politique*
GOOGLE	Representative / Représentant.e	
GOOGLE	Nima BINARA	Counsel / *Conseillère*
ICANN	Amy BIVINS	Legal Counsel / *Conseillère juridique*
ICANN	Elena PLEXIDA	Vice President Government and IGO Engagement / *Vice-présidente chargée de l'engagement des gouvernements et des OIG*
ICANN	Nora MARI	Government and IGO Engagement Manager / *Responsable de l'engagement des gouvernements et des OIG*
IT-Pol Denmark	Jesper LUND	Chairman / *Président*
Kaspersky	Anastasiya KAZAKOVA	Senior Public Affairs Manager / *Responsable principal des affaires publiques*
MARQUES	Clare GRIMLEY	Committee Member, Cyberspace Teal / *Membre du comité, Cyberspace Teal*
Reform ICCLR	Jessica JAHN	Associate / *Associée*

Sapienza University of Rome	Tommaso PIETRRELLA	PHD Student / *Etudiant en doctorat*
University College Dublin Sutherland School of Law	TJ McINTYRE	Associate Professor / *Professeur associé*
University of Oxford	Christopher D'URSO	Rhodes Scholar and Dphil (PhD) in Public Policy Student / *Boursier Rhodes et étudiant en Dphil (doctorat) en politique publique*
University of Maryland Global Campus	Felix URIBE	Adjunct Associate Professor / *Professeur associé adjoint*

CONSULTANTS / *CONSULTANTS*

Betty SHAVE T-CY consultant / *consultante T-CY*
MARCOS SALT T-CY consultant / *consultant T-CY*

COUNCIL OF EUROPE SECRETARIAT / *SECRETARIAT DU CONSEIL DE L'EUROPE*

Patrick PENNINCKX Head of Information Society Department / *Chef du Département de la société de l'Information*	DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME*
Alexander SEGER Executive Secretary of the Cybercrime Convention Committee / *Secrétaire executif du Comité de la Convention sur la Cybercriminalité*	Head of Cybercrime Division / *Chef de la Division Cybercrime* Head of Cybercrime Programme Office (C-PROC) / Chef du Bureau / *Bureau du programme sur la cybercriminalité (C-PROC)* DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME*
Peter KIMPIAN Data Protection Unit / *Unité de Protection des données*	DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME*
Representative / Représentant.e Moneyval / *Moneyval*	DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME*
Nina LICHTNER Programme Officer / *Chargée de programme* Cybercrime Division / *Division de la Cybercriminalité*	DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT - DIRECTION DE L'ACTION CONTRE LE CRIME*

Céline DEWAELE Programme Assistante / *Assistante de programme* Cybercrime Division / *Division de la Cybercriminalité*	DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME*
Floriane SPIELMANN Project Assistant / *Assistante de projet* Cybercrime Division / *Division de la Cybercriminalité*	DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME*
Chloé DUMONT *Trainee / Stagiaire*	DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME*

INTERPRETERS / *INTERPRÈTES*

Chloé CHENETTIER
Sergio Alvarez RUBIO
Hans-Werner MÜHLE
Giamil Ellis LARACUENTE
Stella RAPPOSELLI D'OTTAVIO
Corinne MAGALLON