EUROPEAN
COMMISSION

Brussels, 25.11.2021
COM(2021) 718 final

2021/0382 (NLE)

Proposal for a

COUNCIL DECISION

authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

EXPLANATORY MEMORANDUM

1. THE SUBJECT OF THE PROPOSAL

The present proposal concerns the decision authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence to the Council of Europe 'Budapest' Convention on Cybercrime ('the Protocol').[1] The aim of the Protocol is to provide common rules at international level to enhance co-operation on cybercrime and the collection of evidence in electronic form for criminal investigations or proceedings.

The Commission will also submit a proposal for a Decision of the Council of the European Union ('the Council') authorising Member States to ratify the Protocol in the interest of the European Union.

Cybercrime continues to represent a considerable challenge to our society. Notwithstanding the efforts of law enforcement and judicial authorities, cyberattacks, including ransomware attacks, are increasing and are becoming more complex.[2] In particular the borderless nature of the internet makes cybercrime investigations almost always cross-border in nature, thus requiring close cooperation between authorities in different countries.

Electronic evidence is increasingly important for criminal investigations. The Commission estimates that nowadays law enforcement and judicial authorities need access to electronic evidence in 85% of criminal investigations, including cybercrime.[3] Evidence of any criminal offence is increasingly held in electronic form by service providers in foreign jurisdictions, and an effective criminal justice response requires appropriate measures to obtain such evidence to uphold the rule of law.

Efforts to improve cross-border access to electronic evidence for criminal investigations are undertaken around the globe, at national, at European Union[4] and at international level, including through the Protocol. It is important to ensure compatible rules at international level to avoid conflicts of law when cross-border access to electronic evidence is sought.

2. CONTEXT OF THE PROPOSAL

2.1. Background

The Council of Europe 'Budapest' Convention on Cybercrime (CETS No. 185) ('the Convention') aims at facilitating the fight against criminal offences making use of computer networks. It (1) contains provisions harmonising domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime, (2) provides for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or where the evidence is in electronic form, and (3) aims to set up a fast and effective regime of international cooperation.

---

1 The text of the Protocol will be annexed to the proposal for a Council Decision authorising Member States to ratify, in the interest of the Union, the Protocol.

2 European Union Serious and Organised Crime Threat Assessment 2021 (EU SOCTA 2021).

3 SWD(2018) 118 final.

4 COM(2018)225 and 226 final.

The Convention is open to Member States of the Council of Europe, and non-members upon invitation. Currently, 66 countries are Parties to the Convention, including 26 European Union Member States.[5] The Convention does not envisage that the European Union may accede to the Convention. The European Union is however recognised as an Observer Organisation to the Cybercrime Convention Committee (T-CY).[6]

Notwithstanding efforts to negotiate a new cybercrime convention at the level of the United Nations[7], the Budapest Convention remains the main multilateral Convention for the fight against cybercrime. The Union consistently supports the Convention[8], also in the framework of the financing of capacity building programmes.[9]

Following proposals from the Cloud Evidence Group[10], the Cybercrime Convention Committee adopted several recommendations to address, including through the negotiation of a Second Additional Protocol to the Convention on Cybercrime on enhanced international cooperation, the challenge that electronic evidence relating to cybercrime and other offences is increasingly held by service providers in foreign jurisdictions, while the powers of law enforcement remain limited by territorial boundaries. In June 2017, the Cybercrime Convention Committee approved the Terms of Reference for the preparation of the Second Additional Protocol during the period from September 2017 to December 2019.[11] In view of the need for more time to finalise discussions, as well as the limitations posed by the Covid-19 pandemic in 2020 and 2021, the Cybercrime Convention Committee subsequently extended the terms of reference twice, until December 2020, and subsequently until May 2021.

Following the call from the European Council in its conclusions of 18 October 2018[12], the Commission adopted on 5 February 2019 a Recommendation for a Council Decision authorising the Commission to participate, on behalf of the European Union, in the negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime.[13] The European Data Protection Supervisor adopted an opinion regarding the Recommendation on 2 April 2019.[14] With a decision of 6 June 2019, the Council of the European Union authorised the Commission to participate, on behalf of the European Union, in the negotiations for the Second Additional Protocol.[15]

---

5 All except Ireland, which has signed but not ratified the Convention, but nevertheless committed to pursuing accession.

6 Rules of Procedure of the Cybercrime Convention Committee (T-CY (2013)25 rev), available at www.coe.int/cybercrime.

7 December 2019 United Nations General Assembly (UNGA) Resolution 74/247 on 'Countering the use of information and communications technologies for criminal purposes'.

8 JOIN(2020) 81 final.

9 See for instance the Global Action on Cybercrime Extended (GLACY)+, via https://www.coe.int/en/web/cybercrime/glacyplus.

10 Final report of the Cybercrime Convention Committee's Cloud Evidence Group 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY' of 16 September 2016.

11 https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690

12 https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conslusions/

13 COM(2019) 71 final.

14 EDPS Opinion regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention of 2 April 2019, Opinion 3/2019.

15 Council Decision with reference 9116/19.

As expressed in the 2020 EU Security Union Strategy[16], the 2020 EU Cybersecurity Strategy for the Digital Decade[17] and the 2021 EU Organised Crime Strategy[18], the Commission has been committed to the swift and successful conclusion of the negotiations of the Protocol. The European Parliament also recognised the need to conclude the work on the Protocol in its 2021 Resolution on the EU Cybersecurity Strategy for the Digital Decade.[19]

The Commission participated, on behalf of the European Union, in the negotiations for the Protocol in line with the Decision of the Council of the European Union. The Commission consistently consulted the Council's special committee for the negotiations on the Union position.

In line with the Framework Agreement on relations between the European Parliament and the European Commission[20], the Commission also kept the European Parliament informed of the negotiations by means of written reports and oral presentations.

At the plenary meeting of the Cybercrime Convention Committee of 28 May 2021, the Cybercrime Convention Committee approved the draft Protocol at its level and forwarded the draft for adoption by the Committee of Ministers of the Council of Europe.[21] On 17 November 2021, the Committee of Ministers of the Council of Europe adopted the Protocol.

2.2. The Second Additional Protocol

The aim of the Protocol is to enhance co-operation on cybercrime and the collection of evidence in electronic form of a criminal offence for the purpose of specific criminal investigations or proceedings. The Protocol recognises the need for increased and more efficient co-operation between States and with the private sector, and for greater clarity and legal certainty for service providers and other entities regarding the circumstances in which they may respond to requests from criminal justice authorities in other Parties for the disclosure of electronic evidence.

The Protocol also recognises that effective cross-border cooperation for criminal justice purposes, including between public sector authorities and private sector entities, requires effective conditions and strong safeguards for the protection of fundamental rights. For that purpose, the Protocol follows a rights-based approach and provides for conditions and safeguards in line with international human rights instruments, including the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. As electronic evidence often concerns personal data, the Protocol also includes strong safeguards for the protection of privacy and personal data.

The provisions referred to in the following subparagraphs are of particular importance for the Protocol. The Protocol is accompanied by a detailed explanatory report. Although the explanatory report does not constitute an instrument providing an authoritative interpretation of the Protocol, it is intended to 'guide and assist Parties' in the application of the Protocol.[22]

---

16 COM(2020) 605 final.
17 JOIN(2020) 81 final.
18 COM(2021) 170 final.
19 European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade.
20 Reference L 304/47.
21 https://rm.coe.int/0900001680a2aa42
22 See paragraph 2 of the explanatory report to the Protocol.

2.2.1. Common provisions

Chapter I of the Protocol provides for common provisions. Article 2 determines the scope of application of the Protocol, in line with the scope of the Convention: it applies 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.

In Article 3, definitions are included with regard to 'central authorities', 'competent authorities', 'emergency situations', 'personal data' and 'transferring Party'. These definitions apply to the Protocol, together with definitions included in the Convention.

Article 4 determines the languages in which Parties should submit orders, requests or notifications under the Protocol.

2.2.2. Cooperation measures

Chapter II of the Protocol provides for measures to enhance cooperation. First, Article 5, paragraph 1, determines that Parties shall cooperate on the basis of the Protocol to the widest extent possible. Article 5, paragraphs 2 to 5, determines the application of the measures of the Protocol in relation to existing mutual assistance treaties or arrangements. Article 5, paragraph 7, sets out that the measures in Chapter II shall not restrict cooperation between Parties, or with service providers or entities, through other applicable agreements, arrangements, practices, or domestic law.

Article 6 provides a basis for the direct cooperation between competent authorities in one Party and entities providing domain name registration services in another Party, for the disclosure of domain name registration data.

Article 7 provides a basis for the direct cooperation between competent authorities in one Party and service providers in another Party for the disclosure of subscriber data.

Article 8 provides a basis for enhanced cooperation between authorities for the disclosure of computer data.

Article 9 provides a basis for the cooperation between authorities for the disclosure of computer data in emergency situations.

Article 10 provides a basis for mutual legal assistance in emergency situations.

Article 11 provides a basis for cooperation by video conference.

Article 12 provides a basis for joint investigations and joint investigation teams.

2.2.3. Safeguards

The Protocol follows a rights-based approach with specific conditions and safeguards, some of which are incorporated in the specific cooperation measures, as well as in Chapter III of the Protocol. Article 13 of the Protocol requires Parties to ensure that powers and procedures are subject to an appropriate level of protection for fundamental rights, which, in line with Article 15 of the Convention, ensures the application of the principle of proportionality.

Article 14 of the Protocol provides for the protection of personal data, as defined in Article 3 of the Protocol in line with the Amending Protocol to the Convention for the Protection of

Individuals with Regard to the Processing of Personal Data (CETS 223) (Convention 108+) and Union law.

On that basis, Article 14, paragraphs 2 to 15, set out fundamental data protection principles, including purpose limitation, legal basis, data quality and rules applicable to the processing of special categories of data, obligations applicable to controllers, including on retention, keeping of records, security and as regards onward transfers, enforceable individual rights, including on notification, access, rectification and automated decision-making, independent and effective supervision by one or more authorities as well as administrative and judicial redress. The safeguards cover all forms of cooperation set out in the Protocol, with adaptations where necessary to address the specific features of direct cooperation (e.g. in the context of breach notification). The exercise of certain individual rights can be delayed, limited or refused where necessary and proportionate to pursue important public interest objectives, in particular to prevent risk to an ongoing law enforcement investigations, which is also in line with Union law.

Article 14 of the Protocol should also be read in conjunction with Article 23 of the Protocol. Article 23 strengthens the effectiveness of the safeguards in the Protocol by providing that the Cybercrime Convention Committee will assess the implementation and application of the measures taken in national legislation to give effect to the provisions of the Protocol. In particular, Article 23, paragraph 3 explicitly acknowledges that the implementation by the Parties of Article 14 shall be assessed once ten Parties to the Convention have expressed their consent to be bound to the Protocol.

As a further safeguard, pursuant to Article 14, paragraph 15, where a Party has substantial evidence that another Party is in systematic or material breach of the safeguards set out in the Protocol, it may suspend the transfer of personal data to that Party following consultation (which is not required in case of urgency). Any personal data transferred prior to suspension shall continue to be treated in accordance with the Protocol.

Finally, in view of the multilateral character of the Protocol, Article 14, paragraph 1, point b and point c of the Protocol allow Parties in their bilateral relationships to agree, under certain conditions, on alternative ways to ensure the protection of personal data transferred under the Protocol. While the safeguards of Article 14, paragraphs 2 to 15 apply by default to Parties receiving personal data, on the basis of Article 14, paragraph 1, point b, Parties mutually bound by an international agreement establishing a comprehensive framework for the protection of personal data in line with the applicable requirements of the legislation of the Parties concerned may also rely on that framework. This concerns for instance Convention 108+ (for those Parties that allow data transfers to other Parties under that convention) or the EU-U.S. Umbrella Agreement (within its scope of application, i.e. for the transfer of personal data between authorities and, in combination with a specific transfer arrangement between the U.S. and the EU, for direct cooperation between authorities and service providers). In addition, on the basis of Article 14, paragraph 1, point c, Parties may also mutually determine that the transfer of personal data takes place on the basis of other agreements or arrangements between the Parties concerned. For the EU Member States, such an alternative agreement or arrangement may only be relied upon for data transfers under the Protocol if such transfers comply with the requirements of Union data protection law, namely Chapter V of Directive (EU) 2016/680 (the Law Enforcement Directive) and (for direct cooperation between authorities and service providers under Articles 6 and 7 of the Protocol) Chapter V of Regulation (EU) 2016/679 (the General Data Protection Regulation).

2.2.4. Final provisions

Chapter IV of the Protocol provides for final provisions. Amongst other things, Article 15, paragraph 1, point a, ensures that Parties may establish their relations on the matters set out in the Protocol otherwise, in line with Article 39, paragraph 2, of the Convention. Article 15, paragraph 1, point b, ensures that EU Member States that are Party to the Protocol can continue to apply Union law in their mutual relations. Article 15, paragraph 2, also determines that Article 39, paragraph 3, of the Convention applies to the Protocol.

Article 16, paragraph 3, indicates that the Protocol will enter into force once five Parties to the Convention have expressed their consent to be bound by the Protocol.

Article 19, paragraph 1, provides that Parties may avail themselves of reservations in relation to Article 7, paragraphs 9 point a and 9 point b, Article 8, paragraph 13, and Article 17. Article 19, paragraph 2, provides that Parties may make declarations in relation to Article 7, paragraphs 2, point b, and 8, Article 8, paragraph 11, Article 9, paragraph 1, point b, and 5, Article 10, paragraph 9, Article 12, paragraph 3, and Article 18, paragraph 2. Article 19, paragraph 3, determines that a Party shall make declarations, notifications or communications identified in Article 7, paragraphs 5 point a and point e, Article 8, paragraphs 4 and 10 points a and b, Article 14, paragraphs 7 point c and 10 point b, and Article 17, paragraph 2.

Article 23, paragraph 1, provides a basis for consultations amongst Parties, including through the Cybercrime Convention Committee, in line with Article 46 of the Convention. Article 23, paragraph 2, also provides a basis for the assessment of the use and implementation of the provisions of the Protocol. Article 23, paragraph 3, ensures that the assessment of the use and implementation of Article 14 on data protection shall commence once ten Parties have expressed their consent to be bound by the Protocol.

2.3. Union law and policy in the area

The field governed by the Protocol is largely covered by common rules based on Articles 82(1) and 16 TFEU. The current European Union legal framework includes in particular instruments on law enforcement and judicial cooperation in criminal matters, such as Directive 2014/41/EU regarding the European Investigation Order in criminal matters, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and Council Framework Decision 2002/465/JHA on joint investigation teams. Externally, the European Union has concluded a number of bilateral agreements between the Union and third countries, such as the Agreements on Mutual Legal Assistance between the European Union and the United States of America, between the European Union and Japan and between the European Union and Norway and Iceland. The current European Union legal framework also includes Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'). Member States that participate in the enhanced cooperation should ensure that the EPPO can, in the exercise of its competences as provided for by Articles 22, 23 and 25 of Regulation (EU) 2017/1939, seek cooperation under the Protocol in the same way as national prosecutors of those Member States. These instruments and agreements relate, in particular, to Articles 8, 9, 10, 11 and 12 of the Protocol.

Moreover, the Union has adopted several directives that reinforce procedural rights of suspects and accused persons.[23] These instruments relate, in particular, to Articles 6, 7, 8, 9,

[23] Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings, OJ L 280, 26.10.2010, p. 1; Directive 2012/13/EU of

10, 11, 12 and 13 of the Protocol. One particular set of safeguards concerns the protection of personal data, which is a fundamental right enshrined in the EU Treaties and in the Charter of Fundamental Rights of the European Union. Personal data may only be processed in accordance with the Regulation (EU) 2016/679 (the General Data Protection Regulation) and Directive (EU) 2016/680 (the Law Enforcement Directive). The fundamental right of everyone to the respect for his or her private and family life, home and communications includes the respect for the privacy of one's communications as an essential element. Electronic communications data can only be processed in accordance with Directive 2002/58/EC (the ePrivacy Directive). These instruments relate, in particular, to Article 14 of the Protocol.

Article 14, paragraphs 2 to 15, of the Protocol provides for appropriate data protection safeguards within the meaning of the Union data protection rules, in particular Article 46 of the General Data Protection Regulation and Article 37 of the Law Enforcement Directive, and relevant case law of the European Court of Justice. In line with Union law requirements[24] and in order to guarantee the effectiveness of the safeguards set out in Article 14 of the Protocol, Member States should ensure notification of individuals whose data have been transferred, subject to certain restrictions, e.g. to avoid jeopardising ongoing investigations. Article 14, paragraph 11, point c of the Protocol provides a basis for Member States to fulfil this requirement.

The compatibility of Article 14, paragraph 1, of the Protocol with Union data protection rules also requires that Member States consider the following with regard to possible alternative ways to ensure the appropriate protection of personal data transferred under the Protocol. With regard to other international agreements establishing a comprehensive framework for the protection of personal data in line with the applicable requirements of the legislation of the Parties concerned, under Article 14, paragraph 1, point b, Member States should take into account that, for direct cooperation, the EU-U.S. Umbrella Agreement needs to be complemented with additional safeguards – to be provided in a specific transfer arrangement between the U.S. and the EU/its Member States – that take into account the unique

---

the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, OJ L 142, 1.6.2012, p. 1; Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ L 294, 6.11.2013, p. 1; Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, OJ L 297, 4.11.2016, p. 1; Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings, OJ L 132, 21.5.2016, p. 1; Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016, p. 1; Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings.

[24] See Court of Justice (Grand Chamber), Opinion 1/15, ECLI:EU:C:2017:592, paragraph 220. See also EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), 13 November 2019, p. 6 ("The competent national authorities to whom access to the data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardize the investigations being undertaken by those authorities. … Notification is necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy and their data protection rights in relation to the processing of their data").

requirements of the transfer of electronic evidence directly by service providers rather than between authorities.[25]

Also, under Article 14, paragraph 1, point b, of the Protocol, Member States should consider that, for EU Member States that are Parties to Convention 108+, that Convention by itself does not provide an appropriate basis for cross-border data transfers under the Protocol to other Parties to that Convention. In this respect, they should consider the last sentence of Article 14, paragraph 1, of Convention 108+[26].

Finally, with regard to other agreements or arrangements under Article 14, paragraph 1, point c, Member States should consider that they may only rely on such other agreements or arrangements if either the European Commission has adopted an adequacy decision pursuant to Article 45 of the General Data Protection Regulation (EU) 2016/679 or Article 36 of the Law Enforcement Directive (EU) 2016/680 for the third country concerned that covers the respective data transfers, or if such other agreement or arrangement itself ensures appropriate data protection safeguards pursuant to Article 46 of the General Data Protection Regulation or Article 37, paragraph 1, point a, of the Law Enforcement Directive.

Account must be taken not only of Union law as it currently stands in the area concerned, but also of its future development, in so far as this is foreseeable at the time of analysis. The area covered by the Protocol is of direct relevance to foreseeable future developments of Union law. In this regard, the Commission's proposals on cross-border access to electronic evidence of April 2018 should be noted.[27] These instruments relate, in particular, to Articles 6 and 7 of the Protocol.

The Commission, while participating in the negotiations on behalf of the Union, ensured that the Protocol is fully compatible with Union law and Member States' obligations under it. In particular, the Commission ensured the Protocol provisions allow Member States to respect fundamental rights, freedoms and general principles of Union law as enshrined in the EU Treaties and Charter of Fundamental Rights, including proportionality, procedural rights, the presumption of innocence and the rights of defence of persons subject to criminal proceedings as well as privacy and the protection of personal data and electronic communications data when such data is processed, including transfers to law enforcement authorities in countries outside the European Union, and any obligations incumbent on law enforcement and judicial authorities in this respect. The Commission also took into account the opinion of the European Data Protection Supervisor[28], and of the European Data Protection Board.[29]

---

[25] This is why the Council Decision of 21 May 2019 authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters (9114/19) in its negotiating directives contains a number of additional data protection safeguards. In particular, the negotiating directives stipulate that "[t]he agreement should complement the Umbrella Agreement with additional safeguards that take into account the level of sensitivity of the categories of data concerned and the unique requirements of the transfer of electronic evidence directly by service providers rather than between authorities and transfers from competent authorities directly to service providers."

[26] See also Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018, points 106-107.

[27] COM(2018) 225 and 226 final.

[28] EDPS Opinion regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention of 2 April 2019, Opinion 3/2019.

Furthermore, the Commission ensured that the provisions in the Protocol and the Commission's e-evidence proposals are compatible, including as the draft legislation evolved in the discussions with the co-legislators, and the Protocol does not give rise to conflicts of law. In particular, the Commission ensured that the Protocol includes appropriate data protection and privacy safeguards, which allows EU service providers to comply with their obligations under EU data protection and privacy laws, insofar as the Protocol provides a legal ground for data transfers in reaction to orders or requests issued by an authority from a non-EU Party to the Protocol requiring an EU controller or processor to disclose personal data or electronic communications data.

2.4. Reservations, declaration, notification and communications, and other considerations

The Protocol provides a basis for Parties to avail themselves of certain reservations, and to make declarations, notification or communications in relation to certain articles. Member States should take a uniform approach to certain reservations and declarations, notifications and communications as set out in the Annex to this Decision. To ensure compatibility of the Protocol's implementation with Union law, EU Member States should take the position set out below with respect to those reservations and declarations. Where the Protocol provides a basis for other reservations, declarations, notifications or communications, this proposal authorises Member States to consider and make their own reservations, declarations, notifications or communications.

In order to ensure compatibility between the Protocol's provisions and relevant Union law and policies, Member States should not avail themselves of the reservations pursuant to Article 7, paragraphs 9, point a[30] and point b[31]. In addition, Member States should make the declaration pursuant to Article 7, paragraph 2, point b[32], and the notification pursuant to Article 7, paragraph 5, point a[33]. The absence of these reservations, and the submission of the declaration and notification, are important to ensure compatibility of the Protocol with the Commission's e-evidence legislative proposals, including as the draft legislation evolves in the discussions with the co-legislators.

In addition, in order to ensure a uniform application of the Protocol by EU Member States in their cooperation with Parties that are not EU Member States, Member States are encouraged not to avail themselves of the reservation pursuant to Article 8, paragraph 13[34], also because

---

[29] Including 'EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) of 13 November 2019'; 'Statement 02/201 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) as adopted on 2 February 2021'; 'EDPB Contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime of 4 May 2021'.

[30] Allowing Parties to reserve the right not to apply Article 7 (disclosure of subscriber data).

[31] Allowing Parties to reserve the right not to apply Article 7 (disclosure of subscriber data) to certain types of access numbers if that would be inconsistent with the fundamental principles of its domestic legal system.

[32] Allowing Parties to declare that the order under Article 7, paragraph 1 (disclosure of subscriber data), must be issued by, or under the supervision of, a prosecutor, or other judicial authority, or otherwise be issued under independent supervision.

[33] Allowing Parties to notify the Secretary General of the Council of Europe that when an order is issued under Article 7, paragraph 1 (disclosure of subscriber data), 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.

[34] Allowing Parties to reserve the right not to apply Article 8 (giving effect to orders from another Party) to traffic data.

such a reservation would have reciprocal effect[35]. Member States should make the declaration pursuant to Article 8, paragraph 4, to ensure effect can be given to orders in case additional supporting information is needed, e.g. about the circumstances of the case at hand in order to assess proportionality and necessity.[36]

Member States are also encouraged to refrain from making the declaration under Article 9, paragraph 1, point b,[37] in order to ensure an efficient application of the Protocol.

Member States should make the communications pursuant to Article 7, paragraph 5, point e[38], Article 8, paragraph 10, point a and point b[39], Article 14, paragraph 7, point c, and paragraph 10, point b, to ensure an overall effective application of the Protocol.[40]

Finally, Member States should also take the necessary measures pursuant to Article 14, paragraph 11, point c, to ensure that the receiving Party is informed at the time of transfer of the obligation under Union law to provide notification to the individual to whom the data relates[41], and appropriate contact details to allow the receiving Party to inform the competent authority in the EU Member State once confidentiality restrictions no longer apply and notification can be provided.

2.5. Reason for the proposal

The Protocol will enter into force once five Parties have expressed their consent to be bound by the Protocol in accordance with the provisions of Article 16, paragraphs 1 and 2. The signing ceremony of the Protocol is envisaged to take place in March 2022.

EU Member States should take the necessary steps to ensure swift entry into force of the Protocol, which is important in view of a number of factors.

First, the Protocol will ensure that law enforcement and judicial authorities are better equipped to obtain electronic evidence necessary for criminal investigations. In view of the increasing importance of electronic evidence for criminal investigations, there is an urgent need of law enforcement and judicial authorities to have the right instruments to obtain access to electronic evidence in an effective manner to ensure they can effectively fight crime online.

Second, the Protocol will ensure that such measures to obtain access to electronic evidence will be used in a manner that allow Member States to respect fundamental rights, including

---

[35] See paragraph 147 of the explanatory report to the Protocol that determines that '[a] Party that reserves to this article is not permitted to submit orders for traffic data to other Parties under [Article 8,] paragraph 1'.

[36] Allowing Parties to declare that additional supporting information is required to give effect to orders under Article 8, paragraph 1 (giving effect to orders from another Party).

[37] Allowing Parties to declare that they will not execute requests under Article 9, paragraph 1, point a, (expedited disclosure of computer data in an emergency) seeking only the disclosure of subscriber data.

[38] Allowing Parties to communicate the contact details of the authority that it designates to receive notifications under Article 7, paragraph 5, point a, and perform the actions described in Article 7, paragraph 5, points b, c and d (disclosure of subscriber data).

[39] Allowing Parties to communicate contact information of the authorities designated to submit and to receive orders under Article 8 (giving effect to orders from another Party). In line with requirements under Regulation (EU) 2017/1939, the Member States that participate in the enhanced cooperation on the establishment of the European Public Prosecutor's Office (EPPO) shall include the EPPO in the communication.

[40] Allowing Parties to communicate the authority or authorities that should, respectively, be notified in case of a security incident, or be contacted to seek prior authorisation in case of onward transfers to another State or international organisation.

[41] See above footnote 24.

criminal procedural rights, the right to privacy and the right to the protection of personal data. In the absence of clear rules at international level, existing practices may pose challenges in view of legal certainty, transparency, accountability and respect of fundamental rights and procedural guarantees of the suspects in criminal investigations.

Third, the Protocol will resolve and prevent conflicts of law, affecting both authorities and private sector service providers and other entities, by providing compatible rules at international level for cross-border access to electronic evidence.

Fourth, the Protocol will demonstrate the continued importance of the Convention as the main multilateral framework for the fight against cybercrime. This will be of key importance in the process following the United Nations General Assembly (UNGA) Resolution 74/247 of December 2019 on 'Countering the use of information and communications technologies for criminal purposes' that established an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

3. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- *Legal basis*

The competence of the Union to legislate on matters on the facilitation of the cooperation between judicial or equivalent authorities in relation to proceedings in criminal matters and the enforcement of decisions is based on Article 82(1) TFEU. The competence of the Union for matters on the protection of personal data is based on Article 16 TFEU.

In line with Article 3(2) TFEU the Union has exclusive competence for the conclusion of an international agreement insofar as such conclusion may affect common EU rules or alter their scope. The provisions of the Protocol fall within an area covered to a large extent by common rules as set out in section 2.3 here above.

The Protocol thus falls within exclusive external competence of the Union. The signature of the Protocol by Member States, in the interest of the Union, may thus take place on the basis of Articles 16, 82(1) and 218(5) TFEU.

- *Subsidiarity (for non-exclusive competence)*

Not applicable.

- *Proportionality*

The Union's objectives with regard to this proposal as set out in section 2.5 here above can only be achieved by entering into a binding international agreement providing for the necessary cooperation measures while ensuring appropriate protection of fundamental rights. The Protocol achieves this objective. The provisions of the protocol are limited to what is necessary to achieve its main objectives. Unilateral action does not provide an alternative as it would not provide a sufficient basis for the cooperation with non-EU countries and could not ensure the necessary protection of fundamental rights. Also, adhering to a multilateral agreement such as the Protocol, which the Union has been able to negotiate, is more efficient than entering into negotiations with individual non-EU countries at bilateral level. Under the assumption that all 66 Parties, as well as future new Parties, to the Convention will ratify the Protocol, the Protocol will provide a common legal framework for EU Member States' cooperation with their most important international partners in the fight against crime.

- ***Choice of the instrument***

Not applicable.

4. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- *Ex-post evaluations/fitness checks of existing legislation*

Not applicable.

- *Stakeholder consultations*

The Council of Europe organised six rounds of public consultations in relation to the Protocol negotiations, in July and November 2018, February and November 2019, December 2020, and May 2021.[42] Parties considered the input received as part of these consultations.

The Commission, in its role as negotiator on behalf of the Union, also exchanged views with data protection authorities, and organised targeted consultation meetings throughout 2019 and 2021 with civil society organisations, service providers and trade associations. The Commission took into account the input received from these exchanges.

- *Collection and use of expertise*

In the process of the negotiations, the Commission consistently consulted the Council's special committee for the negotiations in line with the Decision of the Council of the European Union of 6 June 2019 authorising the Commission to participate in the negotiations on behalf of the Union, which provided an opportunity for Member State experts to contribute to the process of the formulation of the Union position. A number of Member State experts also continued to participate in the negotiations, alongside the Commission's participation on behalf of the Union. Stakeholder consultations also took place (see here above).

- *Impact assessment*

An impact assessment was carried out in 2017-2018 to accompany the Commission's e-evidence proposals.[43] In this context, the negotiation for an agreement on a Second Additional Protocol to the Budapest Convention on Cybercrime was part of the preferred option. Relevant impacts are moreover presented in the present explanatory memorandum.

- *Regulatory fitness and simplification*

The Protocol may have implications for certain categories of service providers, including Small and Medium Enterprises (SMEs), as they may be subject to requests and orders for electronic evidence under the Protocol. However, currently, these providers will often already be subject to such requests through other existing channels, sometimes transmitted via different authorities, including on the basis of the Convention[44], other Mutual Legal Assistance treaties, or other frameworks including internet governance multi-stakeholder

[42] https://www.coe.int/en/web/cybercrime/protocol-consultations

[43] SWD(2018) 118 final.

[44] See for instance the Cybercrime Convention Committee Guidance Note 10 of 1 March 2017 on production orders for subscriber information (Article 18 Budapest Convention).

policies.[45] Also, service providers, including SMEs, will benefit from a clear legal framework at international level and a common approach by all Parties to the Protocol.

- *Fundamental rights*

The cooperation instruments under the Protocol are likely to affect fundamental rights where a person's data may be obtained in the context of a criminal proceeding, including e.g. the right to a fair trial, the right to privacy and the right to the protection of personal data. The Protocol follows a rights-based approach and provides for conditions and safeguards in line with international human rights instruments including the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. In particular, the Protocol provides for specific data protection safeguards. Where necessary, the Protocol also provides a basis for Parties to make certain reservations, declarations or notifications, and includes grounds to refuse cooperation in response to a request in specific situations. This ensures compatibility of the Protocol with the EU Charter of Fundamental Rights.

5. BUDGETARY IMPLICATIONS

There are no budgetary implications for the Union budget. Member States may have one-off costs for the implementation of the Protocol and there could be higher costs for authorities of the Member States due to the expected rise in the number of cases.

6. OTHER ELEMENTS

- *Implementation plans and monitoring, evaluation and reporting arrangements*

There is no implementation plan as, following its signature and ratification, Member States will be required to implement the Protocol.

With regard to monitoring, the Commission will take part in the meetings of the Cybercrime Convention Committee, where the European Union is recognised as an Observer Organisation.

[45] See for instance the Resolution of the Board of the Internet Cooperation for Assigned Names and Numbers (ICANN) of 15 May 2019 on the Recommendations on the Temporary Specification for gTLD registration data, available at www.icann.org.

2021/0382 (NLE)

Proposal for a

COUNCIL DECISION

authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16, 82(1) and 218(5) thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) On 9 June 2019, the Council authorised the Commission to participate, on behalf of the Union, in the negotiations for the Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime.

(2) The text of the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (‘the Protocol') was adopted by the Council of Europe Committee of Ministers on 17 November 2021 and is envisaged to be opened for signature in March 2022.

(3) The provisions of the Protocol fall within an area covered to a large extent by common rules within the meaning of Article 3(2) TFEU, including instruments facilitating judicial cooperation in criminal matters, ensuring minimum standards of procedural rights, as well as data protection and privacy safeguards.

(4) The Commission also submitted legislative proposals for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (COM(2018)225 final), and for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings introducing (COM(2018)226 final), binding cross-border European Production and Preservation Orders to be addressed directly to a representative of a service provider in another Member State.

(5) With its participation in the negotiations, on behalf of the Union, the Commission ensured compatibility of the Second Additional Protocol with relevant common European Union rules.

(6) A number of reservations, declarations, notifications and communications are relevant to ensure compatibility of the Protocol with Union law and policies, as well as the uniform application of the Protocol amongst EU Member States in their relation with non-EU Parties, and the effective application of the Protocol.

(7) Given that the Protocol provides for swift procedures that improve cross-border access to electronic evidence and a high level of safeguards, entry into force will contribute to the fight against cybercrime and other forms of crime at global level by facilitating cooperation between the EU Member State Parties and the non-EU Member State

Parties to the Protocol, will ensure a high level of protection of individuals, and will address conflicts of law.

(8) Given that the Protocol provides for appropriate safeguards in line with the requirements for international transfers of personal data under Regulation (EU) 2016/679 and Directive (EU) 2016/680, its entry into force will contribute to the promotion of Union data protection standards at global level, facilitate data flows between the EU Member State Parties and the non-EU Member State Parties to the Protocol, and will ensure compliance of EU Member States with their obligations under Union data protection rules.

(9) The swift entry into force will furthermore also confirm the position of the Council of Europe Budapest Convention as the main multilateral framework for the fight against cybercrime.

(10) The European Union cannot become a Party to the Protocol, as both the Protocol and the Council of Europe Convention on Cybercrime are open to states only.

(11) Member States should therefore be authorised to sign the Protocol, acting jointly in the interests of the European Union.

(12) Member States are encouraged to sign the Protocol during the signing ceremony, or at the earliest possible date thereafter.

(13) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on …

(14) [In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Decision and is not bound by it or subject to its application.]

[OR]

[In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland has notified [, by its letter of ... ,] its wish to take part in the adoption and application of this Decision.]

(15) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Decision and is not bound by it or subject to its application,

HAS ADOPTED THIS DECISION:

Article 1

Member States are hereby authorised to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (‘Protocol’).

Article 2

When signing the Protocol, Member States shall make the reservations, declarations, notifications or communications that are set out in the Annex.

Article 3

This Decision shall enter into force on the day of its adoption.

Article 4

This Decision shall be published in the Official Journal of the European Union.

Article 5

This Decision is addressed to Member States.

Done at Brussels,

For the Council
The President