Council of the European Union

Brussels, 5 September 2025
(OR. en)

12541/25

Interinstitutional Files:
2025/0230 (NLE)
2025/0231 (NLE)

CYBER 235
COPEN 243
JAI 1202
COPS 429
RELEX 1122
JAIEX 94
TELECOM 286
POLMIL 255
CFSP/PESC 1294
ENFOPOL 313
DATAPROTECT 199

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposals for a Council Decision on the signing and conclusion, on behalf of the European Union, of the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes - Opinion of the EDPS

Delegations will find in the Annex the opinion of the European Data Protection Supervisor (EDPS) on the above-mentioned proposals.


EDPS
EUROPEAN DATA PROTECTION SUPERVISOR
The EU's independent data protection authority
Opinion 23/2025
on the two Proposals for Council Decisions on the signing and conclusion of the United Nations Convention against Cybercrime
edps.europa.eu

The European Data Protection Supervisor (EDPS) is an independent institution of the European Union (EU), responsible under Article 52(2) of Regulation (EU) *2018/1725 'With respect to the processing of personal data... for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3) of Regulation* (EU) *2018/1725 '... for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.*

Wojciech Rafał Wiewiórowski was appointed as Supervisor on 5 December 2019 for a term of five years.

Under ***Article 42(1)*** *of Regulation (EU) 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data'.*

This Opinion relates to the Proposal for a Council Decision on the signing, on behalf of the European Union, of the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes[1] *and the Proposal for a Council Decision on the conclusion, on behalf of the European Union, of the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*[2]*. This Opinion does not preclude any future additional comments or recommendations by the EDPS, in particular if further issues are identified or new information becomes available. Furthermore, this Opinion is without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Regulation (EU) 2018/1725. This Opinion is limited to the provisions of the Proposals that are relevant from a data protection perspective.*

[1] COM(2025) 415 final.
[2] COM(2025) 417 final.

1

Executive Summary

On 16 July 2025, the European Commission issued two Proposals for Council Decisions on the signing and conclusion of the United Nations Convention against Cybercrime. The Convention aims to provide common rules at global level to enhance cooperation on cybercrime and the collection of evidence in electronic form for the purpose of criminal investigations or proceedings.

The EDPS is aware that cybercrime is a global and cross-border phenomenon, thus requiring close cooperation between authorities in different countries. The EDPS therefore supports the efforts to devise new models of co-operation, including in the context of co-operation with third countries through international instruments, provided they are compatible with the EU laws and values.

The EDPS recalls the vast number of countries within the United Nations and their highly heterogeneous legal systems as regard the respect of fundamental rights and freedoms, including the fundamental rights to privacy and data protection. Against this background, the EDPS considers of paramount importance to ensure that cooperation with third countries under the Convention does not lead to weakening or otherwise prejudicing the protection of fundamental rights and freedoms of natural persons guaranteed under EU law, in particular their rights to data protection and privacy.

The EDPS positively notes that the Convention expressly states that States Parties are not required to transfer personal data if the data cannot be provided in compliance with their applicable laws concerning the protection of personal data. Member States implementing and applying the Convention should therefore carefully assess whether the conditions of Chapter V of the Law Enforcement Directive are fulfilled before transferring personal data to a third country in each specific case. Member States competent authorities should also carefully consider whether the transfer of personal data to a third country that is Party to the Convention is fully consistent with their own obligations under international human rights law and the fundamental rights and freedoms of the individuals concerned.

Where appropriate, Member States' competent authorities should make use of the grounds to refuse cooperation. Cooperation should be refused, for example, in relation to crimes that are non-existent in their legal system, or if Member States' competent authorities would not be allowed to carry out the action requested with regard to any similar offence under their own jurisdiction, taking into account the relevant case law of the Court of Justice of the European Union. If they do decide to cooperate, Member States competent authorities should make use of the international cooperation mechanism that offers the most robust data protection safeguards in that particular case.

When adopting measures to enable the search and seizure of stored electronic data, Member States should carefully assess the potential impact, in particular on fundamental rights and cybersecurity, of any measure that may result in the weakening or degrading of encryption.

As the protection of personal data is not one of the essential aims or components of the Convention, the EDPS recommends to remove Article 16 of the Treaty on the Functioning of the

European Union as a legal basis for the Proposals to sign and conclude the Convention. Finally, the EDPS recommends to carefully assess the effects of the current text of the Convention in practice and to involve data protection experts in future reviews. Any possible future attempts to include in the Convention offences that are not in line with EU law or values should be strongly opposed.

3

Contents

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union (TFEU),

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ('EUDPR')[3], and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1. On 16 July 2025, the European Commission issued the Proposal for a Council Decision on the signing, on behalf of the European Union, of the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes[4] and the Proposal for a Council Decision on the conclusion, on behalf of the European Union, of the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes[5] ('the Proposals').

2. The objective of the Proposals is to obtain from the Council of the European Union the authorisation for the European Commission to sign and conclude the United Nations Convention against Cybercrime ('the Convention') on behalf of the European Union[6].

3. The Convention aims to provide common rules at global level to enhance cooperation to prevent and combat cybercrime and on the collection of evidence in electronic form for the purpose of criminal investigations or proceedings, creating a basis for cooperation with many countries with whom neither the EU nor its Member States have agreements in place[7]. As such, the Convention is in line with the objectives set out in ProtectEU – the European Internal Security Strategy[8].

4. The United Nations' (UN) General Assembly adopted the text of the Convention and the resolution accompanying it by consensus, on 24 December 2024[9]. The Convention is

[3] OJ L 295, 21.11.2018, p. 39.
[4] COM(2025) 415 final.
[5] COM(2025) 417 final.
[6] See COM(2025) 415 and 417 final, p.1.
[7] See COM(2025) 415 and 417 final, p.2 and Article 1 of the Convention.
[8] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, COM/2025/148 final.
[9] Resolution adopted by the General Assembly on 24 December 2024; A/RES/79/243.

envisaged to be opened for signature in Hanoi, Vietnam on 25 October 2025, and thereafter at United Nations Headquarters in New York until 31 December 2026. The Convention will enter into force once 40 States Parties have expressed their consent to be bound by the Convention in accordance with Article 65, paragraphs 1 and 2, of the Convention.

5. The Convention also provides that a regional economic integration organization, such as the European Union, can sign and ratify the Convention if at least one of the Member States signs and ratifies it[10].

6. On 18 May 2022, the EDPS issued his Opinion 9/2022[11] on the Recommendation for a Council Decision authorising the negotiations for the Convention. The EDPS welcomes that most of the recommendations made in that Opinion have been incorporated or otherwise addressed in the final text of the Convention.

7. The present Opinion of the EDPS is issued in response to a consultation by the European Commission of 16 July 2025, pursuant to Article 42(1) of EUDPR. The EDPS welcomes the reference to this consultation in Recital 18 of the Proposals.

2. General remarks

8. The EDPS understands that cybercrime continues to be a growing threat to the security of citizens and businesses in the European Union and globally, and that electronic evidence is increasingly important for criminal investigations, both into online and traditional crimes[12]. The EDPS is also aware that cybercrime is a global and almost always cross-border phenomenon, thus requiring close cooperation between authorities in different countries. The EDPS therefore supports the efforts to devise new models of co-operation, including in the context of co-operation with third countries through international instruments, provided they are compatible with the EU laws and values.

9. The EDPS recalls that the UN Convention is not the first international instrument for cooperation in the field of cybercrime. The 2001 Council of Europe Convention on Cybercrime (the 'Budapest Convention')[13] already facilitates the fight against criminal offences making use of computer networks. The Budapest Convention is open to Member States of the Council of Europe, as well as non-members upon invitation. To date, it has 80 States Parties, including 26 European Union Member States. Moreover, the Second

[10] See Article 64(4) of the Convention and COM(2025) 415 and 417 final, p.4.
[11] EDPS Opinion 9/2022 on the Recommendation for a Council Decision authorising the negotiations for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, issued on 18 May 2022.
[12] See COM(2025) 415 and 417 final, p.1.
[13] CETS No. 185.

Additional Protocol to the Budapest Convention[14] includes updated rules on the exchange of electronic evidence[15], which, however, are not yet in force[16].

10. The EDPS furthermore notes that the European Union and its Member States are also parties to two of the main United Nations' criminal justice instruments of almost universal adoption, the United Nations Convention against Organised Crime (UNTOC) and the United Nations Convention against Corruption (UNCAC)[17].

11. Pursuant to Article 216(2) TFEU, international agreements concluded by the European Union "*are binding upon the institutions of the Union and on the Member States*". Moreover, according to the settled case law of the Court of Justice of the European Union (CJEU), international agreements become '*an integral part of Community law*'[18] from their coming into force and they have primacy over acts of secondary Union legislation[19].

12. Since the Convention is a binding international instrument, the EDPS reminds that, in line with the case law of the CJEU, the "*obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness*"[20].

13. Transfers of personal data in the context of criminal investigations are liable to have a significant impact on the lives of the individuals concerned, as they will be used in prosecution cases in the receiving country, under its national law. Any interference with the fundamental rights to privacy and data protection guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the EU (the 'Charter'), caused by the application of the Convention, must fulfil the requirements of Article 52(1) of the Charter[21].

14. In this context, the EDPS recalls that the CJEU, in Opinion 1/15 on the international agreement between the EU and Canada regarding the transfer of Passenger Name Records (PNR) data to Canada, found that *"a transfer of personal data from the European Union to a non member country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union"*[22].

---

[14] CETS No. 224.
[15] The Council adopted decisions authorising Member States to sign and ratify the Second Additional Protocol in the interest of the EU: Council Decision (EU) 2022/722 of 5 April 2022 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 (OJ L 134, 11.5.2022, p. 15–20, ELI: http://data.europa.eu/eli/dec/2022/722/oj) and Council Decision (EU) 2023/436 of 14 February 2023 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (OJ L 63, 28.2.2023, p. 48–53, ELI: http://data.europa.eu/eli/dec/2023/436/oj).
[16] The Protocol will enter into force on the first day of the month following the expiration of a period of three months after the date on which five Parties to the Cybercrime Convention have expressed their consent to be bound by the Protocol in accordance with the provisions of Article 16(1) and (2) of the Protocol. Up until the issuing of this Opinion, two Parties have ratified the Protocol.
[17] See COM(2025) 415 and 417 final, p. 3.
[18] Judgment of the Court of Justice of 30 April 1974, *R. & V. Haegeman v. Belgian State*, C-181/73, ECLI:EU:C:1974:41, par. 5.
[19] Judgment of the Court of Justice of 3 June 2008, *Intertanko and Others*, C-308/06, ECLI:EU:C:2008:312, par. 42.
[20] Judgment of the Court of Justice of 3 September 2008, *Kadi and Al Barakaat International Foundation v. Council*, C-402/05 P and C-415/05, ECLI:EU:C:2008:461, par. 285.
[21] See also the EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, issued on 19 December 2019.
[22] Opinion of the Court of Justice of 26 July 2017, *PNR Canada*, ECLI:EU:C:2017:592, par. 214.

15. The EDPS finally recalls the vast number of countries within the UN and their highly heterogeneous legal systems as regard the respect of fundamental rights and freedoms, including the fundamental rights to privacy and data protection. Against this background, the EDPS considers of paramount importance to ensure that cooperation with third countries under the Convention does not lead to weakening or otherwise prejudicing the protection of fundamental rights and freedoms of natural persons guaranteed under EU law, in particular their rights to data protection and privacy. This Opinion aims to provide constructive and objective advice with a view of ensuring that the level of data protection guaranteed by EU law is not undermined.

3. Legal basis

16. According to the Explanatory Memorandum of the Proposals[23], the legal basis for the Proposals are the following provisions of the TFEU: Article 16(2), Article 82(1), Article (83)(1), Article 87(1) and Article 218(5).

17. Article 218 TFEU lays down the procedure for the negotiation and conclusion of agreements between the European Union and third countries or international organisations. Article 82(1) TFEU regulates matters on the facilitation of the cooperation between judicial or equivalent authorities in relation to proceedings in criminal matters and the enforcement of decisions. Article 83(1) TFEU regulates the definition of criminal offences in the area of cybercrime and Article 87(2) TFEU regulates measures concerning law enforcement cooperation.

18. Under Article 16(2) TFEU, the Union has the power to adopt measures relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and by Member States when carrying out activities which fall within the scope of Union law.

19. In line with the jurisprudence of the CJEU, Article 16 TFEU provides an appropriate legal basis in cases where the protection of personal data is one of the essential aims or components of the rules adopted by the EU legislature[24].

20. The EDPS welcomes that the Convention, already in its Preamble, acknowledges the right to protection against arbitrary or unlawful interference with one's privacy, and the importance of protecting personal data. This is a novelty in the UN criminal justice instruments, as the UNTOC and UNCAC do not contain such statements.

21. At the same time, as will be further explained in Section 4.1 of this Opinion, the protection of personal data does not seem to be one of the essential aims or components of the Convention. The Convention contains one provision on personal data protection (Article 36) and this provision mainly consists in preserving domestic legal regimes on the protection of personal data when it comes to transfers of personal data. The Convention itself does not contain any other safeguards specifically for the protection of personal data.

---

[23] See COM(2025) 415 and 417 final, Part 2, p. 6.

[24] See Opinions of the Court of Justice of 6 October 2021, A-1/19 par. 284-285 and of 26 July 2017, *PNR Canada*, ECLI:EU:C:2017:592, par. 96. See also EDPB- EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), issued on 18 June 2021, par. 11.

It is therefore an accessory provision that does not alter the centre of gravity of the Convention which is clearly criminal law matters[25].

22. As the protection of personal data is not one of the essential aims or components of the Convention, the EDPS recommends removing Article 16 TFEU as a substantive legal basis from the Proposals.

4. Relevant safeguards in the Convention

4.1. Article 36 on protection of personal data

23. Article 36 of the Convention provides that States Parties are not required to transfer personal data if the data cannot be provided in compliance with their applicable laws concerning the protection of personal data. States Parties must also ensure that the personal data received in accordance with the Convention are subject to effective and appropriate safeguards. In addition, in case of onward transfers of personal data obtained in accordance with the Convention to a third country or an international organization, the concerned State Party must notify and request the authorization of the original transferring State Party.

24. Even if the scope of Article 36 of the Convention is limited to transfers only, the EDPS positively notes the inclusion of a provision explicitly referring to data protection. As far as the EDPS is aware, this is a novelty in the UN legal framework dealing with cooperation in the criminal justice field and should therefore be welcomed.

25. Transfers of personal data by competent authorities of EU Member States to third country authorities competent in the field of law enforcement are primarily regulated by Directive (EU) 2016/680[26] (the 'LED'), in particular by its Chapter V.

26. In order to ensure that the level of protection of natural persons guaranteed by EU law is not undermined, Chapter V of the LED lays down specific conditions for the transfer of personal data to third countries. The transfer must be based on a transfer instrument, such as an adequacy decision, an instrument ensuring appropriate safeguards (e.g. an international agreement), an assessment by the competent law enforcement authority that such safeguards are ensured in the third country, or, failing the above, one of the derogations available for specific cases (the latter should not be relied upon for systematic sharing of personal data).

27. In the absence of an adequacy decision issued by the European Commission to enable personal data to be transferred to a given third country, transfers of personal data can still

[25] In line with its Article 1, the main purpose of the Convention is the fight against cybercrime and cooperation in the criminal field.
[26] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, pp. 89).

take place if appropriate data protection safeguards are provided in a legally binding instrument[27].

28. As the European Data Protection Board (EDPB) explains in its Guidelines 01/2023 on Article 37 LED, it is important to clarify from the outset what might constitute a legally binding instrument under Article 37(1)(a) LED. First, it should be distinguished between the mere existence of an agreement on cooperation between Parties that entails the exchange of personal data, on the one hand and, on the other hand, the existence of an agreement that regulates the processing of personal data and adduces the necessary safeguards. It is not sufficient to have an agreement in place which provides for a legal basis for the judicial cooperation on criminal matters between the Parties and the inherent data exchanges. Such an agreement does not qualify as a lawful mechanism for the international transfer of personal data under this provision of the LED, unless it contains appropriate data protection safeguards[28].

29. Having this in mind, the EDPS emphasises that, while the Convention itself, as a typical criminal law cooperation instrument, can entail a legal basis for processing in the sense of Article 8 LED, it does not (and does not purport to) provide the necessary appropriate safeguards to serve as a basis for transfer within the meaning of Article 37(1)(a) LED. Therefore, when deciding on a request from a third country, another basis for transfer under Chapter V of the LED should always be identified in order to ensure appropriate data protection safeguards for the transfer of personal data.

4.2. Article 6 on respect for human rights

30. Article 6 of the Convention lays down an overarching requirement for States Parties to respect their obligations under international human rights law when implementing the Convention. Moreover, Article 6 prohibits any interpretation of the Convention permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law. As far as the EDPS is aware, such a provision is also a novelty in the UN legal framework dealing with cooperation in the criminal justice field and should therefore also be welcomed.

31. While a dedicated provision aiming to ensure respect for human rights is indeed a positive development, the EDPS also notes that the requirement for States to implement their obligations under the UN Convention "*consistent with their obligations under international human rights law*" could be implemented differently by States Parties as not all of them have adhered to the same (if any) international agreements providing for the protection of human rights or have implemented the same (or similar) human rights standards.

32. The EDPS therefore calls on the competent authorities of Member States to carefully consider whether the transfer of personal data to a third country that is Party to the Convention is fully consistent with their own obligations under international human rights law and the fundamental rights and freedoms of the individuals concerned.

---

[27] Article 37(1)(a) LED.
[28] EDPB Guidelines 01/2023 on Article 37 Law Enforcement Directive, adopted on 19 June 2024, par. 28.

4.3. Grounds to refuse cooperation

33. Article 40 of the Convention enables States Parties to refuse requests for international cooperation for a variety of reasons, including:

- the absence of dual criminality (Article 40(8));
- if a request for mutual legal assistance is not made in conformity with the provisions of Article 40 (Article 40(21)(a));
- if the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests (which is often internationally interpreted to cover also human rights considerations[29]) (Article 40(21)(b));
- if the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence (Article 40(21)(c));
- if it would be contrary to the legal system of the requested State Party relating to mutual legal assistance (Article 40(21)(d)); and
- if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons (Article 40(22)).

34. The EDPS notes that similar grounds for refusal exist in the Budapest Convention[30] and considers that proper application of these grounds can contribute to the protection of fundamental rights, including the right to the protection of personal data. Notwithstanding this, the EDPS calls on the competent authorities of Member States to carefully scrutinise every request for mutual assistance on a case-by-case basis. Where appropriate, competent authorities should make use of the grounds to refuse cooperation, especially if such cooperation would be incompatible with the fundamental rights, freedoms and general principles of EU law as enshrined in the Treaties and in the Charter.

4.4. Article 24 on conditions and safeguards in national law

35. The EDPS notes that Chapter IV of the Convention, "Procedural Measures and Law Enforcement", prescribes a range of powers and procedures that States Parties must have in place for purposes of investigating and prosecuting cybercrime. Article 24 requires that the establishment, implementation and application in national law of those powers and procedures should be subject to conditions and safeguards. Similarly to Article 6 of the Convention, these safeguards are to be provided by State Parties' domestic law, in accordance with their obligations under international human rights law.

---

[29] See COM(2025) 415 and 417 final, Part 3, p. 10.
[30] See Article 25(4) and 27(4) of the Budapest Convention.

36. The EDPS also notes that Article 23 of the Convention provides that these procedural measures in principle should be available not only for the offenses criminalized under Chapter II of the Convention, but also for other criminal offenses committed by means of an information and communication technology system as well as for the collection of electronic evidence of any criminal offense.

37. The EDPS recalls that, in accordance with CJEU case law, only the objective of fighting serious crime is capable of justifying access by public authorities to personal data retained by service providers *"which taken as a whole, allows very precise conclusions to be drawn concerning the private lives of the persons concerned"*[31]. Where such conclusions cannot be drawn and therefore access could not *"be defined as a serious interference with the fundamental rights of the persons whose data is concerned"*, the Court further held that *"the interference that access to such data entails is capable of being justified by the objective of (...) preventing, investigating, detecting and prosecuting 'criminal offences' generally without it being necessary that those offences be defined as 'serious'"*[32].

38. The EDPS therefore reminds that any establishment, implementation and application of powers and procedures in national law of Member States, must fully comply with EU law and CJEU jurisprudence. In addition, when assessing a request emanating from a third country that is a State Party to the Convention, Member States' competent authorities should carefully assess the subject matter of the request, as well as conditions and safeguards provided for in a specific third country. Where relevant, Member States should use the possibility to refuse cooperation in accordance with Articles 36 and 40 of the Convention, including the possibility to refuse such cooperation if the authorities of the requested State Party would be prohibited by their domestic law from carrying out the action requested with regard to any similar offence[33]. In this regard, the EDPS welcomes that the Convention, in its Article 2 (c), (d) and (f) distinguishes between specific data categories that may be the subject matter of a request, similarly to the Budapest Convention and Regulation (EU) 2023/1543[34] (the 'e-Evidence Regulation'), as this should contribute to ensure legal certainty for all stakeholders involved[35].

5. Scope of the Convention

5.1. Criminal offences covered by the Convention

39. In his Opinion 9/2022, the EDPS recommended limiting the scope of the international cooperation provisions to crimes defined in the Convention, as this would constitute an important additional guarantee of the necessity and proportionality of the measures provided for by the Convention, having in mind the highly heterogeneous legal systems of the possible future Parties to the Convention[36]. However, Article 40(1) of the Convention

[31] Judgment of the Court of Justice of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, par. 54, see also par. 56.
[32] *Ibid*, par. 62.
[33] Article 40(21)(c) of the Convention. See also Section 4.3. of this Opinion.
[34] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, pp. 118).
[35] See EDPS Opinion 9/2022, par. 34.
[36] See EDPS Opinion 9/2022, par. 24.

provides for the possibility for mutual legal assistance in investigations, prosecutions and judicial proceedings not only in relation to the offences established in accordance with the Convention, and for the purposes of the collection of evidence in electronic form of offences established in accordance with the Convention, but also for (other) serious crimes.

40. While the EDPS would have preferred the scope of the cooperation under the Convention to be limited to crimes defined in the Convention, the EDPS is also aware that this "expanded" scope for cooperation is not entirely new in international criminal law instruments.

41. In this regard, the EDPS positively notes that the scope of cooperation under the Convention is actually more limited than the one provided for in the Budapest Convention as the cooperation under the Convention is limited to serious crimes[37] only, while the Budapest Convention allows for cooperation for the collection of evidence in electronic form for any type of crime[38].

42. Even though the scope of cooperation under the Convention is limited to serious crimes only, the EDPS recommends that, before cooperating with third countries, Member States' competent authorities, carefully analyse what constitutes a 'serious crime' in the third country in question. Where relevant, Member States should make use the possibility to refuse cooperation in accordance with Article 40 of the Convention. In particular, they should refuse cooperation for crimes that are non-existent in the EU and Member States legal systems, or if they would be prohibited by their domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction.

5.2. Excluding direct access to data and direct cooperation with service providers by law enforcement authorities

43. In his Opinion 9/2022, the EDPS recommended that the EU should oppose any provisions in the Convention that would provide for cross-border direct access to data or cross-border direct cooperation with service providers, as the EDPS considers cross-border direct access to data by law enforcement authorities of third countries as a particularly intrusive measure and consequently having a bigger impact on the fundamental rights to privacy and data protection[39].

44. In that sense, the EDPS is satisfied that the Convention does not provide for any provisions on direct cross-border access to data or direct cross-border cooperation with service providers.

---

[37] Article 2(h) defines "serious crime" as conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty. It should also be noted that the e-Evidence Regulation, considers as "serious crime" offences that carry at least a three-year maximum custodial sentence (see recital 40 and Article 5). In this sense, the Convention provides a higher threshold for the definition of a serious crime.
[38] See Article 25(1) of the Budapest Convention.
[39] See EDPS Opinion 9/2022, par. 26.

6. Search and seizure of stored electronic data

45. Article 28(4) of the Convention provides that each State Party must adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the information and communications technology system in question, the information and telecommunications network, or their component parts, or measures applied to protect the electronic data therein, to provide, as is reasonable, the necessary information to enable the undertaking of the measures referred to in paragraphs 1 to 3 of that Article.

46. The EDPS observes that Article 28(4) of the Convention may result in States Parties imposing obligations upon third parties, such as communication services providers to effectively provide competent authorities with access to encrypted communications[40].

47. In that regard, the EDPS recalls that the CJEU has considered that data security measures play a key role to ensure that the essence of the fundamental right to the protection of personal data in Article 8 of the Charter is not adversely affected[41]. In addition, in the case of *Podchasov v. Russia*[42], the European Court of Human Rights (ECtHR) considered that an "*obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued*".

48. In the digital age, technical solutions to secure and protect the confidentiality of electronic communications, including measures for encryption, are key to ensure the enjoyment of all fundamental rights[43]. The EDPS therefore calls on Member States to carefully consider the potential impact, in particular on fundamental rights and cybersecurity, of any measures that might result in the weakening or degrading of encryption[44]. In particular, Member States should abstain from imposing any obligations that would weaken data security for all users of an electronic communications service.

7. List of competent authorities

49. In his Opinion 9/2022, the EDPS recommended that the Convention be accompanied by an exhaustive list of competent authorities in the receiving countries to which data would be transferred as well as a short description of their competences[45].

---

[40] It should be noted that the Budapest Convention contains a similar provision (Article 19(4)). Paragraph 202 of the Explanatory Report to the Budapest Convention notes that "*The information that can be ordered to be provided is that which is necessary to enable the undertaking of the search and seizure, or the similarly accessing or securing. The provision of this information, however, is restricted to that which is "reasonable". In some circumstances, reasonable provision may include disclosing a password or other security measure to the investigating authorities. However, in other circumstances, this may not be reasonable; for example, where the disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched.*"

[41] Judgment of the Court of Justice of 8 April 2014, *Digital Rights Ireland and Seitlinger and others*, C-293/12 and C-594/12, par. 40.

[42] ECtHR judgment of 13 February 2024, 33696/19, § 79.

[43] See Human Rights Council, Resolution 47/16 on the promotion, protection and enjoyment of human rights on the Internet, UN Doc. A/HRC/RES/47/16 (26 July 2021).

[44] See also EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, adopted on 28 July 2022, par. 13.

[45] See EDPS Opinion 9/2022, par. 38.

50. The EDPS considered this as a useful safeguard in order to enable EU authorities to easily identify to which specific authorities the data would be transferred and to ensure that they would also be competent for the purposes of the transfer.

51. The EDPS notes that Article 40(12) of the Convention provides that each State Party shall designate a central authority or authorities that would have the responsibility and power to receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution. In addition, Article 40(15)(b) requires that a request for mutual assistance also contains "the name and functions of the authority conducting the investigation, prosecution or judicial proceeding". The EDPS considers that this information should enable Member States' central authorities to easily identify to which specific authorities data would be transferred and to ensure that they would also be competent for the purposes of the transfer.

8. Relationship with other instruments

52. The Convention is not the first and only international instrument for cooperation in the field of cybercrime. Already in his Opinion 9/2022, the EDPS recommended that other agreements with third countries should apply *in lieu* of the Convention, should these agreements ensure higher standards with regard to the protection of fundamental rights, in particular the right to privacy and data protection, and that it should be ensured that, between EU Member States, EU secondary law still applies in order to preserve the EU legal order[46].

53. The EDPS welcomes Article 60 of the Convention, which confirms that States Parties that have already concluded an agreement or treaty on the matters dealt with in the Convention, or have otherwise established their relations on such matters, or should they in future do so, are entitled to apply that agreement or treaty or to regulate those relations accordingly.

54. In addition to the application of EU secondary law between themselves, the EDPS recommends Member States to use the cooperation mechanism that offers the most robust data protection safeguards when cooperating with third countries.

9. Review of the Convention

55. The EDPS notes Article 57 of the Convention, which establishes a Conference of the States Parties to the Convention, a body that should convene no later than one year after the entry in force of the Convention. Amongst other, the Conference must review periodically the implementation of the Convention and make recommendations for improvement, as well as considering possible supplementation or amendment of the Convention.

[46] See EDPS Opinion 9/2022, par. 21-22.

56. The EDPS welcomes this possibility for review of the practical implementation of the Convention and recommends including data protection experts, including representatives of national data protection authorities, in these reviews.

10. Additional protocols to the Convention

57. Point 5 of the Resolution A/79/460[47], tied to the Convention, requires the UN ad hoc Committee to already begin negotiating a supplementary protocol that would include additional criminal offenses. The Committee would hold two sessions of a duration of 10 days each, with the first session taking place two years after the adoption of the Convention by the General Assembly and the second session in the following calendar year.

58. The EDPS would like to caution against rushing into the start of negotiations for expanding the scope of the Convention before having carefully assessed the effects of the current text of the Convention in practice.

59. In addition, if the negotiations were to start in the near future and the EU is to join these future negotiations, the EU should strongly oppose any possible attempt to include in the Convention offences that are not in line with the EU laws or values.

11. Conclusions

60. In light of the above, the EDPS recommends to remove Article 16 TFEU as a legal basis for the Proposals.

61. In addition, the EDPS makes the following recommendations to Member States implementing and applying the Convention:

(1) before transferring personal data to a third country that is a State Party to the Convention, Member States' competent authorities should carefully assess whether the conditions of Chapter V of the LED are fulfilled (as the Convention does not provide the necessary appropriate safeguards to serve as a basis for transfer within the meaning of Article 37(1)(a) LED);

(2) where appropriate, Member States' competent authorities should make use of the grounds to refuse cooperation, in line with Articles 36 and 40 of the Convention. In particular, Member States competent authorities should refuse cooperation in relation to crimes that are non-existent in their legal system, or if they would be prohibited by their domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction;

[47] Resolution A/79/460 of 27 November 2024.

(3) *when adopting measures to enable the search and seizure of stored electronic data, Member States should carefully assess the potential impact, in particular on fundamental rights and cybersecurity, of any measure that may result in the weakening or degrading of encryption;*

(4) *when handling a third country request for international cooperation, Member States competent authorities should carefully consider whether the transfer of personal data to a third country that is Party to the Convention is fully consistent with their own obligations under international human rights law and the fundamental rights and freedoms of the individuals concerned and make use of the international cooperation mechanism that offers the most robust data protection safeguards in that particular case;*

(5) *to involve data protection experts, including representatives of national data protection authorities, in the reviews of the Convention.*

62. Finally, the EDPS recommends to carefully assess the effects of the current text of the Convention in practice and oppose any attempts to include in the Convention offences that are not in line with EU law or values.

Brussels,

17