



EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data
protection authority

18 May 2022

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

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation (EU) 2018/1725 '[w]ith 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)'...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' and under Article 57(1)(g), the EDPS shall 'advise on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data'.*

This Opinion relates to the EDPS' mission to advise the EU institutions on coherently and consistently applying the EU data protection principles, including when negotiating agreements with third countries in the law enforcement sector. It builds on the general obligation that international agreements must comply with the provisions of TFEU and the respect for fundamental rights that stands at the core of EU law. In particular, compliance with Articles 7 and 8 of the Charter of Fundamental Rights of the EU and Article 16 TFEU must be ensured.

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 Recommendation that are relevant from a data protection perspective.

Executive Summary

On 29 March 2022, the European Commission issued a Recommendation for a Council Decision authorising the participation of the Commission, on behalf of the European Union, in the United Nations (UN) negotiations for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

The EDPS understands the need for law enforcement authorities to secure and obtain electronic evidence quickly and effectively. He underlines however, that there is already a similar international instrument in force i.e. the Budapest Convention and its Second Additional Protocol which is now open for signature.

The EDPS notes that negotiations in the UN for another convention aiming to address cybercrime and cross-border cooperation in criminal matters have already started. He therefore supports the recommendation for the Commission to be authorised to negotiate on behalf of the EU, as it would contribute to better preserving the level of protection guaranteed by the EU data protection framework. The EDPS notes, however, the vast numbers of countries within the UN, with highly heterogeneous legal systems. Against this background, the EDPS considers that there is a substantial risk that the final text of the Convention could lead to a weakening of the fundamental rights and freedoms of natural persons provided for by EU law, in particular their rights to data protection and privacy. Therefore, it has to be underlined that should the Council authorise the Commission to negotiate in this framework on behalf of the EU, such authorisation would not require the EU to become party to the Convention, should it be adopted. The EDPS considers that the EU should not seek to be party to such a Convention, should the level of data protection of natural persons guaranteed by EU law be undermined.

This Opinion aims to provide constructive and objective advice to the EU institutions with a view to ensuring that the level of data protection as guaranteed by EU law is not undermined. The EDPS welcomes that the mandate aims at ensuring from the outset that the Convention provides strict conditions and strong safeguards to ensure that EU Member States can respect and protect fundamental rights, freedoms and general principles of EU law as enshrined in the EU Treaties and the Charter of Fundamental Rights of the EU.

In this context, the EDPS stresses the need to ensure in particular full respect for the fundamental rights to privacy and to the protection of personal data. The EU data protection law regime provides, in principle, that data transfers to a third country can take place without additional requirements only when that third country ensures an adequate level of protection. When the third country has not been declared as adequate, exceptions apply for specific transfers, as long as appropriate safeguards are provided. While the EDPS recognises that it may not be feasible to replicate the terminology and definitions of EU law in an agreement with a large number of third countries, the safeguards for individuals must be clear and effective in order to fully comply with EU law. The Court of Justice of the European Union in recent years has reaffirmed data protection principles including judicial redress and individual rights of individuals. These principles become all the more important considering the sensitivity of the data required for criminal investigations.

Against this background, the EDPS considers that, while many negotiating directives already envisaged are welcome, they should be reinforced. In particular, to ensure compliance with the EU Charter and Article 16 TFEU, the EDPS makes four main recommendations on the negotiating directives:

-to limit the international cooperation provisions to the crimes defined in the Convention;

-direct access to data by third country law enforcement authorities and cross-border direct cooperation with service providers should be excluded;

-to ensure that future bilateral and multilateral agreements with third countries should apply in lieu of the Convention should these future agreements ensure higher standards with regard to the protection of fundamental rights, in particular the right to privacy and data protection;

-to ensure that the Convention shall not have effect between two Contracting States if one of them makes the notification that the ratification, acceptance, approval or accession of another Contracting State will not have the effect of establishing relations between those two Contracting States pursuant to this Convention.

Additionally, the Opinion offers further recommendations for improvements and clarifications of the negotiating directives. The comments in this Opinion are without prejudice to any additional comments that the EDPS could make as further issues may arise and would then be addressed once further information is available. He expects to be consulted later on the provisions of the draft Convention before its finalisation.

TABLE OF CONTENTS

1. Introduction.....	5
2. General remarks	7
3. Relationship with other instruments.....	8
4. Scope of the Convention	10
4.1. Criminal offences covered by the Convention.....	10
4.2. Excluding direct access to data and direct cooperation with service providers by law enforcement authorities	10
5. Need for appropriate safeguards regarding international data transfers and the respect of fundamental rights.....	11
6. Suspension, review of the Convention and establishment of relations pursuant to the Convention	13
7. Conclusions.....	14

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data¹ ('the EUDPR'), and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1. The United Nations (UN) is an intergovernmental organisation, currently made up of 193 Member States². The UN and its work are guided by the purposes and principles contained in its founding Charter. Pursuant to the UN Charter, the organisation's objectives include maintaining international peace and security, protecting human rights, delivering humanitarian aid, promoting sustainable development, and upholding international law³.
2. On 17 December 2018, the UN General Assembly adopted Resolution 73/187 on 'Countering the use of information and communications technologies for criminal purposes'⁴. Subsequently, on 27 December 2019, it adopted Resolution 74/247⁵ through which it decided to establish an open-ended ad hoc Intergovernmental committee of experts ('the Ad Hoc Committee'), to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. Resolution 74/247 stresses the need to enhance coordination and cooperation among States in combating the use of information and communications technologies for criminal purposes, including by providing technical assistance to developing countries, upon their request. The Resolution also stresses the need to improve national legislation and frameworks and build the capacity of national authorities to deal with such use in all its forms, including its prevention, detection, investigation and prosecution⁶, **taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes**, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on

¹ OJ L 295, 21.11.2018, p. 39.

² See the UN Member States here: <https://www.un.org/en/about-us/member-states>

³ See Preamble of the Charter of the United Nations, San Francisco, 26 June 1945: <https://www.un.org/en/about-us/un-charter/full-text>

⁴ United Nations General Assembly Resolution of 17 December 2018, [A/RES/73/187](https://www.un.org/en/assembly/resolutions/73/187).

⁵ United Nations General Assembly Resolution of 27 December 2019, [A/RES/74/247](https://www.un.org/en/assembly/resolutions/74/247).

⁶ See page 1 of the Resolution.

Cybercrime⁷. Three EU Member States (Estonia, Poland and Portugal) are Vice-Chairs within the Ad Hoc Committee⁸.

3. On 26 May 2021, by Resolution 75/282⁹, the UN General Assembly further reaffirmed that the Ad Hoc Committee shall **take into full consideration existing international instruments** and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes¹⁰. It decided that this Ad Hoc Committee shall convene at least six sessions, and conclude its work in order to provide a draft Convention to the General Assembly at its seventy-eighth session, which should start in September 2023 and end in September 2024.
4. The first negotiating session was held from 28 February until 11 March 2022. At that occasion the objectives, scope, structure and key elements of the Convention were discussed¹¹. According to the draft report of this first negotiating session, it was agreed that the following elements should form the structure of the Convention¹²:

Preamble

1. General provisions
 2. Criminalization
 3. Procedural measures and law enforcement
 4. International cooperation
 5. Technical assistance, including exchange of experience
 6. Preventive measures
 7. Mechanism of implementation
 8. Final provisions.
5. The European Commission took part in the meetings of the Ad Hoc Committee as an observer. An intersessional session took place on 24 and 25 March 2022 to solicit inputs from a diverse range of stakeholders on the elaboration of the draft Convention¹³. The next negotiating session should start on 30 May 2022¹⁴.
 6. On 29 March 2022, the European Commission issued a Recommendation for a Council Decision authorising the participation of the Commission, on behalf of the European Union, in the United Nations negotiations for a comprehensive international Convention on countering the use of information and communications technologies for criminal purposes

⁷ The open-ended intergovernmental [Expert Group](#) to Conduct a Comprehensive Study on Cybercrime was established by the Vienna-based Commission on Crime Prevention and Criminal Justice (CCPCJ) on the request of the UN General Assembly [Resolution 65/230](#), and is a subsidiary body of CCPCJ. The Expert Group is separate from the Ad Hoc Committee negotiating the Convention, which is a subsidiary body of the General Assembly with a different mandate.

⁸ Members of the Ad Hoc Committee are as follows: Algeria (Chair), Egypt, Nigeria, China, Japan, Estonia, Poland, Russian Federation, Dominican Republic, Nicaragua, Brazil, Australia, Portugal, United States (Vice-Chairs), Indonesia (rapporteur).

⁹ United Nations General Assembly Resolution of 26 May 2021, [A/RES/75/282](#).

¹⁰ See point 11 of the Resolution.

¹¹ Submissions to this first session are available here: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.

¹² <https://documents-dds-ny.un.org/doc/UNDOC/LTD/V22/012/09/PDF/V2201209.pdf?OpenElement>.

¹³ https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/intersessional-consultations/1st-intersessional-consultation.

¹⁴ https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.

(‘the Recommendation’)¹⁵. The Recommendation is accompanied by an Annex (‘the Annex’), which sets out the proposed Council directives to negotiate the Convention.

7. The Commission recommends the adoption of a Council Decision on the basis of the procedure laid down in Article 218 of the Treaty on the Functioning of the European Union (TFEU) for agreements concluded between the EU and third countries. With this Recommendation, the Commission seeks to obtain authorisation from the Council to be appointed as the main negotiator on behalf of the EU in order to ensure the appropriate participation of the EU in the UN negotiations which are expected to touch upon elements that relate to EU legislation and competence, notably in the area of cybercrime¹⁶.
8. The present Opinion of the EDPS is issued in response to a consultation by the European Commission of 29 March 2022, pursuant to Article 42(1) of EUDPR. The EDPS welcomes the reference to this consultation in Recital 5 of the Recommendation.

2. General remarks

9. According to the Explanatory Memorandum, negotiations on the Convention are expected to relate to common EU rules to fight cybercrime, such as Directive 2011/93/EU on combating the sexual exploitation of children online and child pornography, Directive 2013/40/EU on attacks against information systems, and Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment¹⁷. Other EU instruments provide common rules for fighting crimes that may be enabled by the use of information systems, such as terrorism, trafficking in human beings, illicit drug trafficking, illicit arms trafficking, money laundering, corruption and organised crime¹⁸. The negotiations are also expected to cover criminal procedural and cooperation measures. The Union has adopted several instruments in this area¹⁹.
10. The EDPS notes that the negotiations within the UN are already engaged in accordance with the previously mentioned Resolution 74/247 and Resolution 75/282 of the UN General Assembly. Given the relevance of these negotiations for EU policy in the area of cybercrime and collecting electronic evidence in criminal matters, in particular for the protection of personal data and privacy, the EDPS **supports the adoption of a Council Decision giving a clear mandate to the European Commission** to participate in these negotiations on behalf of the EU.
11. As underlined by the Recommendation²⁰, a new international convention on countering the use of information and communications technologies for criminal purposes may affect common Union rules or alter their scope. The EDPS stressed the need to ensure that the

¹⁵ 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 (COM(2022)132 final).

¹⁶ See Explanatory Memorandum, p. 2 and Article 1 of the Recommendation.

¹⁷ See Explanatory Memorandum, p. 3.

¹⁸ *Idem*.

¹⁹ *Idem*, p. 4.

²⁰ See Recital 3.

Convention is compatible with EU law, including compliance with the Charter, in particular the rights to privacy and to protection of personal data, and with Article 16 TFEU.

12. The EDPS understands the need for law enforcement authorities to secure and obtain electronic evidence quickly and effectively. He recalls, however, the vast number of countries within the UN, with highly heterogeneous legal systems. Against this background, the EDPS considers that there is a substantial risk that the Convention could lead to a weakening of the protection of fundamental rights and freedoms of natural persons guaranteed under EU law in particular their rights to data protection and privacy.
13. The EDPS also underlines that there is already a similar international instrument in force i.e. the Budapest Convention and its Second Additional Protocol which has recently been negotiated and is now open for signature.
14. Against this background, the EDPS wishes to stress that the Council authorisation of the Commission to negotiate on behalf of the EU should not be construed as a requirement for the EU to become party to the Convention, should it be adopted, and in particular, that **the EU should not seek to become a party to such a Convention if it could undermine the level of data protection of natural persons guaranteed by EU law.**
15. While the EDPS recognises that it may not be feasible to replicate the terminology and definitions of EU law in an agreement with a vast number of third countries, the safeguards for individuals must be clear and effective in order to fully comply with EU law. The Court of Justice of the European Union in recent years has reaffirmed data protection principles including judicial redress and individual rights of individuals. These principles become all the more important considering the sensitivity of the data required for criminal investigations.
16. This Opinion aims to provide constructive and objective advice with a view of ensuring the level of data protection as guaranteed by EU law is not undermined. It provides further recommendations on the following topics:
 - the relationship between the Convention and other instruments;
 - the scope of the Convention;
 - the safeguards regarding the international transfers of personal data;
 - the final clauses of the Convention (suspension, review and establishment of relations).
17. The EDPS remains at the disposal of the Commission, the Council and the European Parliament to provide advice at further stages of this process.

3. Relationship with other instruments

18. The Recommendation²¹ recalls that a binding international instrument requiring its parties to lay down specific criminal offences committed against or by means of electronic

²¹ See Explanatory Memorandum, p. 1.

networks in their national law, entailing minimum requirements on investigative powers available in a criminal investigation and fostering international co-operation between the Parties, already exists, namely, **the Council of Europe Convention on Cybercrime (ETS No. 185) ('the Budapest Convention')**, which is open for signature by Member States of the Council of Europe and by non - members which have participated in its elaboration or for accession (upon invitation), for those non-members which have not participated to its elaboration. Currently, 66 countries are Parties to the Budapest Convention, including 26 European Union Member States²² and other third countries members of the Council of Europe such as Armenia, Azerbaijan or Turkey as well as countries who are not members of the Council of Europe, such as Australia, Canada, Ghana, Israel, Japan, Morocco, Paraguay, Philippines, Senegal, Sri Lanka, Tonga or the United States²³. In addition, on 17 November 2021, the Committee of Ministers of the Council of Europe adopted a Second Additional Protocol to the Budapest Convention which has been opened for signature since 12 May 2022. The Protocol aims to provide for additional tools for international cooperation, including for co- operation in emergency situations.²⁴

19. The EDPS **welcomes point 6 of the Annex** recommending the Union to achieve that the future UN Convention “is **compatible with and complement[s] existing** international instruments, in particular the 2001 Council of Europe Budapest Convention on Cybercrime and its protocols, the 2000 United Nations Convention against Transnational Organized Crime and its protocols, but also other relevant international and regional instruments”²⁵ and that the future UN Convention “**avoids any impact on their application** or the further accession of any country to them and, to the extent possible, avoid unnecessary duplication”²⁶.
20. The EDPS also **welcomes point 17 of the Annex** according to which the Union should achieve that the “**cooperation measures [...] are compatible with such conventions and with international human rights standards**” and **point 23** of the Annex, where it is made clear that the Union should aim to achieve that the Convention **preserves existing global and regional instruments**.
21. The EDPS however **recommends** including in the Annex that the Union should aim to achieve **that future agreements with third countries should apply in lieu of the Convention should these future agreements ensure higher standards with regard to the protection of fundamental rights, in particular the right to privacy and data protection**²⁷.

²² All except Ireland, which has signed but not ratified the Convention, but nevertheless committed to pursuing accession.

²³ See the Chart of signatures and ratification of the Cybercrime Convention for a complete and updated list of countries parties to the Cybercrime Convention, available at: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>

²⁴ On 5 April 2022, the Council of the European Union adopted a decision authorising Member States to sign, in the interest of the EU, the Second Additional Protocol. On the same day, the Council also decided to send to the Parliament for its approval the decision to authorise member states to ratify the Protocol.

²⁵ Emphasis added.

²⁶ Emphasis added.

²⁷ See for instance [Council decision authorising the opening of negotiations to amend the Agreement between the European Union and Japan on mutual legal assistance in criminal matters](#) (12141/21) and [Council decision authorising the opening of negotiations with a view to concluding 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).

22. Finally, the EDPS welcomes and strongly supports the inclusion of a “**disconnection clause**” in point 23 of the Annex to ensure that between EU Member States, EU secondary law still applies in order to preserve the EU legal order.

4. Scope of the Convention

4.1. Criminal offences covered by the Convention

23. The EDPS welcomes the objective of **clearly and narrowly defining** offences that would be subject to the Convention, i.e. “offences that can only be committed using information systems” (**point 9** of the Annex) and “offences that can be committed without using information systems but that can be enabled by the use of information systems in certain circumstances, **but only in cases where the involvement of information systems substantially changes the characteristics or impact of the offences** (**point 10** of the Annex) [emphasis added]. He also welcomes that the definitions should be “compatible with those in other relevant international or regional conventions in particular in the area of organised crime or cybercrime, and international human rights standards” (**point 11** of the Annex).
24. Under **point 16 of the Annex**, it is recommended that the Convention provides for “*cooperation measures that allow authorities in different States that are party to the instrument to cooperate effectively for the purpose of criminal investigations or proceedings concerning offences defined in the instrument **or** to cooperate to preserve or obtain electronic evidence of **any** criminal offence as part of a criminal investigation or proceeding*” [emphasis added]²⁸. The EDPS observes that the recommended directives encompass cooperation to preserve or obtain electronic evidence of any criminal offence as part of criminal investigations or proceedings. He considers that limiting the scope of the international cooperation under the Convention only to the crimes defined by the Convention would constitute an important guarantee of the necessity and proportionality of the proposed solutions, having in mind highly heterogeneous legal systems of the possible future parties to the Convention. Therefore, the **EDPS considers that the scope of the future provisions on cooperation should also be limited to the crimes defined in the Convention.**

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

25. At this early stage of the negotiations, the scope of the Convention still remains unclear, in particular as far as the modalities of cooperation are concerned.
26. However, as the EDPS already stated in the framework of the negotiations of the Second Additional Protocol to the Budapest Convention²⁹, he 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. Hence, he **considers that the such provisions should not be**

²⁸ Emphasis added.

²⁹ [EDPS Opinion 3/2019 regarding the participation in the negotiations in view of a second additional Protocol to the Budapest Cybercrime Convention](#), paragraphs 18 and 19.

introduced in the Convention and a directive to this effect should be introduced in the Annex.

27. Given the number of countries likely to become parties to the Convention, with highly heterogeneous legal systems as regard the respect of fundamental rights and freedoms, including the fundamental rights to privacy and data protection, the EDPS also recommends opposing any attempt to introduce in the Convention of provisions on direct cooperation by third countries authorities with service providers under EU jurisdiction. In this regard, **it should be clarified that point 15 of the Annex concerns only the cooperation between the law enforcement authorities and service providers in the same country** and does not concern cross-border cooperation between law enforcement authorities and service providers in another country. This need for clarification is all the more important as point 19 of the Annex states that the Convention should ensure that EU Member States are able to comply with requirements for the international transfers of personal data within the meaning of the GDPR, which seems to imply that direct cooperation between service providers in the EU and third countries authorities parties to the Convention is in fact not excluded at this stage.

5. Need for appropriate safeguards regarding international data transfers and the respect of fundamental rights

28. The EDPS recalls that, 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 CJEU, international agreements become from their coming into force *'an integral part of Community law'*³⁰, and they have primacy over acts of secondary Union legislation³¹.
29. Since the Convention would be a binding international instrument to which the Union would be a party³², the EDPS notes 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'*³³. **It is therefore essential to ensure that the obligations stemming from the Convention fully respect the fundamental right to data protection.**
30. The EDPS therefore welcomes **point 8 of the Annex** stipulating that the Union should achieve that the provisions of the Convention achieve the highest possible protection of human rights and that EU Member States should be able to comply with EU law, including the fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and the Charter. The EDPS also welcomes in this regard the clear reference to the **principle of proportionality in point 13 of the Annex.**

³⁰ Judgment of the Court of Justice of 30 April 1974, C-181/73, R.&V. *Haegeman v. Belgian State*, ECLI:EU:C:1974:41, paragraph 5.

³¹ Judgment of the Court of Justice of 3 June 2008, C-308/06, *Intertanko and Others*, ECLI:EU:C:2008:312, paragraph 42.

³² See point 25 of the Annex.

³³ Judgment of the Court of Justice of 30 April 1974, *Joined cases C-402/05 P and C-415/05 P, Kadi v. Council*, ECLI:EU:C:2008:461, paragraph 285.

31. In addition, the EDPS notes and **supports point 18 of the Annex** which aims to achieve that cooperation measures are subject to the conditions provided for by the law of the requested party and provide for broad grounds for refusal such as to ensure the protection of fundamental rights, including the right to the protection of personal data, including in the context of personal data transfers, and, where appropriate, the existence of double criminality.
32. The EDPS recalls that according to the 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*”³⁴. 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’*”³⁵.
33. Therefore, to comply with Article 52(1) of the Charter, the EDPS considers that the categories of data for which the production and transfer of personal data could be ordered must be proportionate to the types of offences concerned. **In particular, it should be ensured that only serious crimes could justify the exchange of data entailing a serious interference with the fundamental rights to data protection and privacy.**
34. In addition, the EDPS welcomes point 15 of the Annex, recommending that the Union should aim to achieve that the procedural measures to preserve or obtain electronic evidence contain a clear and narrow definition of the type of information covered and stresses the importance of laying down clear and straightforward definitions of data categories in the UN Convention in order to ensure legal certainty for all stakeholders involved. **The EDPS recommends ensuring a clear delineation between data categories; such a delineation would contribute to ensuring legal certainty.**
35. The EDPS welcomes and **underlines the importance of point 19 of the Annex**. This point states first that **the Convention should provide for strict conditions and strong safeguards** to ensure that EU Member States can respect and protect the fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and the Charter including, in particular, the principle of proportionality, the right to effective judicial redress, **the right to privacy, the right to the protection of personal data and of electronic communications data** when such data is processed, **including for transfers to authorities in countries outside the European Union**. Second, it specifies that the Convention should ensure that EU Member States **are able to comply with requirements for the international transfers of personal data within, in particular, the meaning of the Directive (EU) 2016/680**³⁶ (‘the LED’) and **Directive 2002/58/EC**³⁷.

³⁴ 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.

³⁵ *Ibid* par. 62. [Emphasis added].

³⁶ 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, p. 89.

³⁷ Emphasis added.

36. In the specific context of transfers of personal data for law enforcement purposes by EU law enforcement authorities, the EDPS recalls that pursuant to Article 37 and Recital 71 of the LED that transfers not based on an adequacy decision should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards exist. Such legally binding instruments could be legally binding agreements which could be enforced by the data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. The controller should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, the controller should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. The controller should be able to require additional safeguards.
37. In this regard, the EDPS **expresses strong doubts whether the future Convention could provide a stand-alone basis for transfers of personal data in accordance with EU law** and therefore recommends making sure that Member States are able to invoke and impose additional safeguards so that transfers taking place in the context of this Convention would only be those in line with EU law, including EU secondary law.
38. Finally, the EDPS would like to further stress that the specific authorities in the third countries to which data would be transferred and which would process these data should be clearly defined in order to ensure that they are also competent for the purposes of the transfer. In that sense, therefore, the EDPS **recommends that the Convention be accompanied by an exhaustive list of the competent authorities in the receiving countries to which data would be transferred as well as a short description of their competences. This should also be reflected in one of the directives of the Annex.**

6. Suspension, review of the Convention and establishment of relations pursuant to the Convention

39. The EDPS welcomes the insertion of a specific provision **allowing for suspension** of the Convention modelled where possible and appropriate along the provisions of other relevant international or regional conventions in particular in the area of organised crime or cybercrime³⁸. The EDPS **recommends** in this regard to **further specify** that the Union should aim to achieve that **a Contracting State may** at the time of signature, ratification or accession, **declare that it will not execute a request for the transfers of personal data to another party, should there be indications³⁹ that an essential level of protection of the data is no longer ensured in the requesting State.**

³⁸ See point 24 of the Annex

³⁹ Such as the suspension from the UN Human Rights Committee.

40. The EDPS also **recommends** that the Annex provide for requesting the introduction of a clause setting out the **mandatory periodical review** of the practical operation of the Convention. To ensure a meaningful review, it should be provided for at the latest five years after its entry into force and then at regular intervals, specifying the frequency of these additional reviews. The content of the review should be specified. The review should focus not only on the implementation of the Convention but also assess the necessity and proportionality. The review teams should include data protection experts including representatives of national data protection authorities.
41. Finally, given the highly heterogeneous nature of the countries likely to be party to the Convention, the EDPS **recommends including in the mandate that the Union should aim at ensuring that the Convention shall not have effect between two Contracting States if one of them makes the notification** that the ratification, acceptance, approval or accession of another Contracting State shall **not** have the effect of establishing relations between those two Contracting States pursuant to this Convention⁴⁰.

7. Conclusions

42. The EDPS **supports** the adoption of a Council Decision giving a clear mandate to the European Commission to participate in the UN ongoing negotiations for this Convention, on behalf of the EU. However, he stresses that an authorisation to participate to the negotiations should not require the EU to be party to the Convention should it be adopted, and in particular, the EU should not seek to be party to such Convention should the level of data protection of natural persons guaranteed by EU law be undermined.
43. The EDPS welcomes and underlines the importance of points 6, 17 and 23 of the Annex aiming at preserving existing global and regional instruments, and of the safeguards included in points 8, 9, 10, 11, 13, 18, 19 and 24 of the Annex.
44. In light of the above, the EDPS makes the following recommendations:

Concerning the relationship between the Convention and other instruments

-) including in the mandate that the Union should aim to achieve that future agreements with third countries should apply in lieu of the Convention, should these future agreements ensure higher standards with regard to the protection of fundamental rights, in particular the right to privacy and data protection.

Concerning the scope of the Convention

-) limiting the cooperation provisions to the crimes defined in the Convention.
-) making clear in the mandate that the Union should oppose any provisions on cross-border direct access to data and cross-border direct cooperation with service providers.

⁴⁰ See for instance the [Hague Convention on the recognition and enforcement of foreign judgments in civil or commercial matters](#), The Hague, 2 July 2019, Article 29.

- J clarifying that the directives under point 15 of the Annex do not concern cross-border cooperation.

Concerning the need for appropriate safeguards and the respect of fundamental rights

- J making clear in the mandate that the Union should ensure a clear delineation between data categories.
- J including a directive in the mandate to aiming at achieving that the Convention is accompanied by an exhaustive list of the competent authorities in the receiving countries to which data would be transferred as well as a short description of their competences.

Concerning the final clauses of the Convention:

- J further specifying in the mandate that the Union should aim to achieve that a Contracting State may at the time of signature, ratification or accession, declare that it will not execute a request for the transfers of personal data to another party, should there be indications that an essential level of protection of the data is no longer ensured in the requesting State.
- J including in the mandate that the Union should aim at achieving the introduction of a clause setting out the mandatory periodical review of the practical operation of the Convention. It should be provided for at the latest five years after its entry into force and then at regular intervals, specifying the frequency of these additional reviews. The content of the review should be specified. The review should focus not only on the implementation of the Convention but assess the necessity and proportionality. The review teams should include data protection experts, including representatives of national data protection authorities.
- J including in the mandate that the Union should aim at ensuring that the Convention shall not have effect between two Contracting States if one of them makes the notification that the ratification, acceptance, approval or accession of another Contracting State will not have the effect of establishing relations between those two Contracting States pursuant to this Convention.

45. Finally, the EDPS remains at the disposal of the Commission, the Council and the European Parliament to provide advice at further stages of this process. The comments in this Opinion are without prejudice to any additional comments that the EDPS could make as further issues may arise and would then be addressed once further information is available. He expects to be consulted on the provisions of the draft Convention before its finalisation.

Brussels, 18 May 2022

(e-signed)

Wojciech Rafał Wiewiórowski