
**EUROPEAN DATA PROTECTION SUPERVISOR**

The EU's independent data protection authority

20 January 2022

# Opinion 1/2022

on the two Proposals for Council Decisions authorising Member States to sign and to ratify, 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

edps.europa.eu

*The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 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)'...for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.*

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

*Under* ***Article 42(1)*** *of Regulation 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.*

**Executive Summary**

On 25 November 2021, the Commission adopted two Proposals for Council Decisions, under Articles 16, 82(1) and 218(5) and (6) of the Treaty on the Functioning of the European Union, one authorising Member States to sign and the other to ratify, in the interest of the European Union, the Second Additional Protocol to the Budapest Convention on Cybercrime. The Annex to the Proposals sets out the Council's directives for the reservations, declarations and communications, when signing and ratifying the Protocol.

Investigating and prosecuting crime is a legitimate aim, and international co-operation including information exchange has become more important than ever. As the EDPS has long argued, the EU needs sustainable arrangements for sharing personal data with third countries for law enforcement purposes, fully compatible with the EU Treaties and the Charter of Fundamental Rights. Even when investigating domestic cases, law enforcement authorities increasingly find themselves in 'cross-border situations' because information is stored electronically in a third country. The growing volume of requests and the volatility of digital information put a strain on existing models of co-operation, such as MLATs. The EDPS understands that authorities face a race against time to obtain data for their investigations and supports efforts to devise new models of co-operation, including in the context of co-operation with third countries.

The Protocol aims to improve the traditional co-operation channels and includes provisions to enhance direct co-operation between law enforcement authorities and service providers in a cross-border context. In particular, the Protocol would enhance co-operation on cybercrime and the collection of evidence in electronic form concerning criminal offences for the purpose of specific criminal investigations or proceedings.

While recognising that it is not possible to replicate entirely the terminology and definitions of EU law in a multilateral international agreement, the EDPS underlines that the appropriate safeguards for individuals must be ensured in order to fully comply with EU law.

Data protection principles including fairness, accuracy and relevance of information, independent oversight and individual rights of individuals are as relevant for public bodies as they are for private companies. These basic principles are all the more important considering the sensitivity of the data required for criminal investigations.

This Opinion aims to provide objective analysis and constructive advice to the EU institutions as the Council is examining the Commission's Proposals to sign and ratify the Protocol and before the European Parliament is called to provide its consent to the conclusion of the Protocol.

The EDPS welcomes that no provision on direct access to data by law enforcement authorities has been included in the final text of the Protocol. He also welcomes that the Protocol contains a dedicated Article on the protection of personal data. In addition, the EDPS notes positively the many safeguards that have been included in the Protocol.

The EDPS understands that it is confirmed that the EU-US Umbrella Agreement would apply to transfers from the EU to the United States of America in the framework of the provisions set out in the Protocol related to the co-operation between authorities. The EDPS regrets such outcome.

Should a Council Decision be adopted authorising the Member States to, respectively sign and ratify, in the interest of the Union, the Protocol, the EDPS welcomes the proposals of the Commission for the Member States to make, in the interest of the Union, the declaration, notification and communication under Article 7(2)(b), (5)(a) and (e) of the Protocol. These proposals ensure that service providers in the Union may be requested the transfer of personal data only on the basis of orders issued, in the requesting third country Party to the Protocol, by, or under the supervision of, a prosecutor or other judicial authority, or under independent supervision and under the control of a competent authority within the requested Member State.

The EDPS also notes positively the proposal that Member States make the declaration under Article 8(4) of the Protocol (on the co-operation between competent authorities to give effect to production orders of subscriber information and traffic data), so as to ensure that additional supporting information is required to give effect to orders under this provision.

In addition, the EDPS has the following recommendations in relation to the future Council Decisions, should the Protocol be signed and ratified by the Member States, in the interest of the Union:

- Certain data contained in the category of subscriber information within the meaning of the Cybercrime Convention, may be deemed under EU law as traffic data entailing a serious interference with the fundamental rights of the data subject, access to which may be justified only by the fight against serious crime. Therefore, the EDPS recommends Member States, contrary to the proposal of the Commission, to reserve the right not to apply Article 7 of the Protocol on disclosure of subscriber data by service providers directly to competent authorities of another country in relation to certain types of access numbers, pursuant to Article 7(9)(b);

- Member States should designate, pursuant to Article 7(5)(e) of the Protocol, a judicial or other independent authority;

- The proposed communication by the Member States to the United States authorities, at the time of signature or when depositing their instrument of ratification, acceptance or approval, in relation to the EU-US Umbrella Agreement should be clarified;

- The proposed consideration, in relation to other agreements or arrangements under Article 14(1)(c) of the Protocol that could replace the data protection provision of the Protocol (Article 14), should be amended.

# Table of contents

**THE EUROPEAN DATA PROTECTION SUPERVISOR,**

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[1],

Having regard to Regulation (EC) No 2018/1725 of the European Parliament and of the Council of 23 October2018 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 data[2], and in particular Articles 42(1), 57(1)(g) and 58(3)(c) thereof,

Having regard to 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[3],

**HAS ADOPTED THE FOLLOWING OPINION:**

# 1. Introduction and background

1. In June 2017, the Cybercrime Convention Committee of the Council of Europe approved the Terms of Reference for the preparation of a Second Additional Protocol to the Convention on Cybercrime during the period from September 2017 to December 2019[4].

2. On 5 February 2019, the Commission adopted a Recommendation[5] for a Council Decision to authorise the participation of the Commission, on behalf of the European Union, in the negotiations on a Second Additional Protocol (hereinafter 'the Protocol')[6] to the Council of Europe Convention on enhanced international co-operation on cybercrime and electronic evidence (hereinafter the 'Cybercrime Convention') (CETS No. 185)[7].

3. The European Data Protection Supervisor (hereinafter 'the EDPS') adopted an Opinion regarding the Recommendation on 2 April 2019[8]. By 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 in view of the Protocol[9].

4. The Cybercrime Convention Committee extended the terms of reference twice, until December 2020, and subsequently until May 2021. The Protocol was prepared by the Cybercrime Convention Committee (T-CY) between September 2017 and May 2021. Over ninety sessions of the T-CY Protocol Drafting Plenary, Drafting Group and Sub-groups as well as six rounds of stakeholder consultations were held in this period.

5. The European Data Protection Board contributed to the public consultations on the draft Protocol on 13 November 2019, 2 February 2021 and 4 May 2021[10].

6. The European Parliament recognised the need to conclude the work on the Protocol in its 2021 Resolution on the EU Cybersecurity Strategy for the Digital Decade[11].

7. On 17 November 2021, the Committee of Ministers of the Council of Europe adopted the Protocol. It should be opened for signature in May 2022. Amendments to it may therefore only be proposed by a Party to the Protocol and adopted by the Committee of Ministers. The Protocol requires acceptance of all Parties for the amendments to come into force[12].

8. The European Union cannot become a Party to the Protocol, as both the Protocol and the Cybercrime Convention are open to States only[13].

9. On 25 November 2021, the Commission adopted two Proposals for Council Decisions, under Articles 16, 82(1) and 218(5) and (6) of the Treaty on the Functioning of the European Union (TFEU)[14].

10. According to these Proposals[15], the Protocol falls within an area covered to a large extent by common rules within the meaning of Article 3(2) TFEU. The Commission seeks to obtain, with these Proposals, two Decisions from Council authorising Member States to respectively sign and ratify, in the interest of the European Union, the Protocol. Both Proposals are accompanied by an Annex (hereinafter 'the Annex') which provides instructions for Member States, regarding the reservations, declarations, notifications or communications and other considerations to be made, when signing and ratifying, in the interest of the European Union, the Protocol. The Proposal relating to the ratification is also accompanied by the text of the Protocol in Annex.

11. In order for the agreement to be concluded, should the Council decide to authorise its signature by the Member States, in the interest of the Union, the Council should adopt a decision authorising the Member States, in the interest of the Union, to ratify the agreement, after obtaining the consent of the European Parliament. 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[16].

12. The EDPS has been consulted on both Proposals by the European Commission following their adoption, pursuant to Article 42(1) of Regulation (EU) No 2018/1725. Reference to this Opinion is made in Recitals 12 and 13 of the Proposals on the ratification and the signature of the Protocol respectively. He wishes to underline that this Opinion is without prejudice to any additional comments that the EDPS could make on the basis of further available information.

## 2. Objectives of the Second Additional Protocol

13. The Cybercrime 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 (hereinafter 'the Member States')[17] 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 States[18].

14. The Cybercrime Convention is a binding international instrument requiring the Parties to lay down specific criminal offences committed against or by means of electronic networks in their national law and to establish specific powers and procedures enabling their national authorities to carry out their criminal investigations, including for collecting evidence of an offence in electronic form. The Convention entails minimum requirements on investigative powers available in a criminal investigation and fosters international co-operation between the Parties. In particular, its Chapter III on international co-operation[19] contains both general provisions on international co-operation, that may also be found in other treaties on co-operation in criminal matters, as well as provisions that are specific to the collection of electronic evidence.

15. The Protocol aims to provide for additional tools, including for co-operation in emergency situations, as further detailed below. The Protocol is accompanied by an explanatory report[20] which reflects the understanding of the drafters. Although it 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[21].

16. The Protocol includes:

    - Provisions **allowing for direct co-operation between competent authorities** in one Party on the one hand, and entities providing **domain name registration services or service providers** in another Party on the other hand, for respectively, the disclosure of **domain name registration data or subscriber information**[22] (Articles 6 and 7).

    - Provisions **enhancing international co-operation between authorities**:

        - giving effect to **orders for expedited production of subscriber information and traffic data**[23] (Article 8);

        - **non-binding requests** for the **expedited disclosure of stored computer data**[24] **in an emergency** (Article 9);

        - **emergency mutual legal assistance** (Article 10[25]);

        - video conferencing (Article 11);

    - Joint investigations and joint investigation teams (Article 12);

    - **Safeguards** (Articles 13 and 14), **including data protection requirements**. Specific conditions and safeguards are also incorporated in the specific co-operation measures.

17. Direct co-operation requests for the disclosure of domain name registration data (Article 6) and the requests for the expedited disclosure of stored computer in an emergency (Article 9) are *non-binding* requests[26].

18. The Protocol provides for the **possibility for a Party to *reserve the right not to apply***:

    – Article 7 (direct co-operation for disclosure of subscriber information) in its entirety or, if disclosure of certain types of access numbers under this article would be inconsistent with the fundamental principles of its domestic legal system, not to apply this article to such numbers (Article 7(9))[27].

– Article 8 (enhancing international co-operation between authorities giving effect to orders for expedited production of subscriber information and traffic data) to traffic data (Article 8(13))[28].

19. The Protocol also foresees the **possibility for a Party *to make certain declarations***, among which the following declarations:

– under Article 7 (direct co-operation for disclosure of subscriber information) allowing the requested Party to require that when an order is issued to a service provider in its territory:

  - such order to be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision (paragraph 2 (b)).

  - simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigations or proceeding of an authority which may instruct the services providers not to disclose the subscriber information if certain conditions or grounds of refusal are met (paragraph 5 (a) and (e)).

– under Article 8 (expedited production of subscriber information and traffic data) allowing the requested Party to require that additional supporting information is required to give effect to orders (paragraph 4).

20. In the proposed Council Decisions, the Commission proposes that the Member States be authorised to sign and ratify the Protocol, acting jointly in the interest of the Union, with a number of reservations and declarations. In particular, **Member States are instructed to refrain from reserving the right not to apply Article 7 as a whole** or in relation to certain types of access numbers[29] and are encouraged to refrain from reserving the right not to apply Article 8 (giving effect to orders for subscriber information and traffic data from another Party) in relation to traffic data pursuant to Article 8(13). The proposed Council Decision does, however, **instruct the Member State to avail themselves of the above-mentioned declarations under Articles 7 and 8 so that the additional safeguards contained therein would be applicable**[30].

## 3. General comments

21. The EDPS understands that authorities face a race against time to obtain data for their investigations and supports efforts to devise new models of co-operation, including in the context of co-operation with third countries. In this regard, he recalls his call together with the EDPB for a new generation of mutual legal assistance treaties ('MLAT') to be implemented, allowing for a much faster and secure processing of requests in practice[31].

22. 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 from their coming into force '*an integral part of Community law*'[32], and they have primacy over acts of secondary Union legislation[33].

23. Since the Cybercrime Convention, as well as any of its additional protocols, is a binding international instrument, 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*'[34]. It is therefore essential to ensure that the obligations stemming from the Protocol would not prejudice these principles as far as data protection is concerned.

24. The Protocol which the Commission proposes to sign and ratify would allow inter alia transfers of personal data both from Member States' competent authorities[35] and from private entities in the Member States[36] and the subsequent processing of such data by the third country authorities Party to the Protocol and private entities in such country.

25. In this regard, Recitals 8 of both Proposals state that '*[g]iven 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*'.

## 3.1. On the processing, by an authority of a Member State or a private entity in the territory of a Member State[37], of personal data received under the Protocol

26. Article 14 of the Protocol concerns the protection of personal data. Paragraph (1)(e) of that provision provides that nothing in that Article - '*shall prevent a Party from applying stronger safeguards to the processing by its own authorities of personal data received under this Protocol*'. Member States would therefore be allowed to apply stronger safeguards to the processing, by their authorities or a private entity in their territory, of personal data received under the Protocol.

## 3.2. On the transfers to third countries Parties to the Protocol

27. The EDPS notes that under Articles 6 and 7, the Protocol allows for transfers of personal data by private entities, pursuing a law enforcement objective, which objective is different from the one for which the data were collected.

28. As a preliminary matter, the EPDS notes that the 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 (hereinafter 'the Charter'), enabled by the Protocol must fulfill the requirements of Article 52(1) of the Charter.

29. Transfers from a law enforcement authority to a service provider or an entity providing domain name registration services in a third State must comply with the data protection principles laid down in Directive (EU) 2016/680 ('LED')[38], in particular those provided for in Chapter V of the Directive, in order to ensure that the level of protection of natural persons guaranteed by EU law is not undermined.

30. In accordance with Article 44 of Regulation (EU) 2016/679 ('GDPR')[39], it should be assessed whether the Protocol ensures that transfers by private entities in the context of Articles 6 and 7 of the Protocol, may take place under the conditions set out in Chapter V of the GDPR, subject to the other provisions of the Regulation (see section 4).

31. When it comes to the transfer, by private entities in the EU, of data required by a judgment or a decision of an authority from a third country, it stems from Article 48 GDPR, that such judgment or decision '*may only be recognised or enforceable in any manner if based on an*

*international agreement, such as a [MLAT], in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to [Chapter V]'* of the GDPR.

32. In July 2017, the CJEU delivered Opinion 1/15[40] on the international agreement between the EU and Canada regarding the transfer of Passenger Name Records (PNR) data to Canada, in which it sets out the conditions under which an international agreement can provide a legal basis for transfers of personal data falling within the scope of Directive 95/46/EC (now replaced by the GDPR). The CJEU 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*'[41]. **It follows from Opinion 1/15 that the level of protection resulting from the Protocol for the exchange of personal data with third countries should be essentially equivalent to the level of protection provided for in EU law.** In this regard, the EDPS points out that according to the case law of the CJEU, both Articles 7 and 8 of the Charter have to be assessed in conjunction with the **right to effective remedy enshrined in Article 47 of the Charter**[42].

33. As regard the legal basis, under Article 6 of the Protocol, the requests issued under the Protocol for domain name registration information are the basis for a voluntary co-operation and are therefore not binding, under the Protocol, on the requested entity. The Protocol leaves it to the Parties to determine the form of implementation[43]. As for orders under Article 7, the Protocol requires that Parties adopt such measures as necessary for service providers in their territory to respond to an order issued by a competent authority in another Party. The explanatory report indicates in this regard that '*[t]he form of implementation depends on Parties' respective legal and policy considerations*'[44].

34. For Member States, this would include providing, according to the explanatory report, '*a clear basis for the processing of personal data. In view of additional requirements under data protection laws to authorise eventual international transfers of the responsive subscriber information, the Protocol reflects the important public interest of this direct co-operation measure and includes safeguards required for that purpose in Article 14*'. The GDPR provides for some possible legal basis in such cases[45] and the Protocol does not prevent the domestic law from further specifying the legal basis for transfers as long as it allows for the co-operation the Protocol provides for[46].

# 4. On the safeguards regarding international data transfers and respect of fundamental rights

## 4.1. Status of the Protocol as far as data protection is concerned

35. While all Member States are parties to the Convention 108[47] of the Council of Europe which is applicable in the law enforcement area, not all third countries parties to the Cybercrime Convention are parties to the Convention 108[48]; only a minority benefits from an adequacy decision under the GDPR[49] and only one (the United Kingdom) benefits from an adequacy decision under the LED.

36. Given the law enforcement context and the potential risks that such transfers of data could pose to data subjects, the safeguards included in this Protocol with third countries should satisfactorily address and mitigate these risks.

37. **Article 14** of the Protocol on the protection of personal data provides safeguards **in relation to the data received under the Protocol**, including the data as part of an order or a request under the Protocol, so as '*to permit Parties to meet [the data protection] requirements*' in relation to transfers of personal data for the purposes of the Protocol[50]. In this regard, the EDPS notes positively that the concept of personal data as defined in Article 3 of the Protocol is 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.

38. It would be up to the law enforcement authorities of the Member States to assess the proportionality of their requests or orders under the Protocol[51]. Equally, it would be up to such authorities to assess whether their requests or orders for the production of personal data to a third country Party to the Protocol comply with the requirements of EU law before sending a request or an order.

39. According to Article 14(1)(d), '*each Party shall consider that the processing of personal data pursuant to paragraphs [2 to 15 of Article 14] meets the requirements of its personal data protection legal framework* ***for international transfers of personal data****, and no further authorisation for transfer shall be required under that legal framework. A Party may only refuse or prevent data transfers to another Party under this Protocol for reasons of data protection under the conditions set out in paragraph 15 [...]*'[52].

40. This means that if Member States are Party to the Protocol, they recognise that said Protocol provides appropriate safeguards for the transfer of personal data. It therefore needs to be assessed whether appropriate safeguards are provided in the context of this Protocol for transfers by law enforcement authorities or private entities in a Member State.

41. In this regard, it is the understanding of the EDPS that Article 14(1)(d) means that Member States are prohibited to refuse or prevent the transfer of the requested data for reasons related to the application of their own **legal framework for international transfers of personal data** even in a specific case. In other words, additional specific conditions to transfers of personal data may not be invoked as a ground to refuse or prevent a transfer to a Party to the Protocol as such. However, should there be a need for additional safeguards in a specific case, the Protocol provides for avenues to ensure additional safeguards under Chapter II (Measures for enhanced co-operation) (see section 4.4.). Finally, it must be underlined that only a valid request under the Protocol, which complies inter alia with the requirements set forth in Articles 13 and 14, may trigger the obligation to assist the requesting Party and hence to transfer data.

## 4.2. Principle of proportionality

42. **Article 13** of the Protocol requires, in accordance with Article 15 of the Cybercrime Convention[53], which refers expressly to the application of the principle of proportionality, '*Parties to ensure that the establishment, implementation and application of the powers and procedures provided for in this Protocol are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties*'. It applies to all the provisions of the Protocol.

43. The EPDS also notes positively that **Article 14(2)(b)** provides that in seeking and processing personal data[54], '*the receiving Party shall ensure under its domestic law that personal data sought and processed are relevant to and not excessive in relation to the purposes of such processing*'[55]. While the Protocol does not further specify what 'relevant and not excessive' means, paragraph 231 of the explanatory report clarifies that this requirement may be implemented via '*the principles of necessity and proportionality*'.

44. In addition, **Article 14(2)(a)** specifies that '*the Party that has received personal data shall process them for the purposes described in Article 2*[56]*. It shall not further process the personal data for an incompatible purpose, and it shall not further process the data when this is not permitted under its domestic legal framework*'. It stems in particular from Article 2 of the Protocol as further explained in the explanatory report that the provisions of the Protocol may not be used for mass or bulk production of data[57].

45. Furthermore, as mentioned above, Chapter II of the Protocol (Measures for enhanced co-operation) provides for additional avenues to implement the proportionality principle.

46. It is the opinion of the EDPS that, the application of this principle[58] and the possibility to refuse partly or totally to comply with a request under the Protocol based on proportionality stem also from this Chapter, which provides for the possibility to add conditions to the supply of the requested information[59] or grounds of refusals under Articles 7, 8 and 10, such as Article 27(4) of the Cybercrime Convention[60].

## 4.3. Protection of personal data

47. Article 14, paragraphs 2 to 15, sets out fundamental data protection principles, which cover all forms of co-operation set out in the Protocol.

48. These principles cover those provided for by the GDPR and the LED: purpose limitation, data minimisation, accuracy, security, and integrity, sensitive data, obligations applicable to controllers (on retention and storage limitation, automated decision-making, records and logging, and as regards onward sharing and onward transfers), individual rights (on transparency and notice, access, rectification, including erasure) and judicial and non-judicial remedies and independent and effective oversight by one or more authorities (see section 5).

### 4.3.1. Purpose limitation and data minimisation principles

49. As mentioned above, **transfers of personal data by a law enforcement authority of a Member State** to a third country may take place if it is necessary for the purposes of the investigation, detection or prosecution of criminal offences.

50. In this regard, according to **Article 2** of the Protocol, the measures described in the Protocol shall be applied '*to **specific** criminal investigations or proceedings concerning criminal offences related to computer systems and data, and to the collection of evidence in electronic form of a criminal offence; and as between Parties to the First Protocol that are Parties to this Protocol, to **specific** criminal investigations or proceedings concerning criminal offences established pursuant to the First Protocol*'[61].

51. This objective falls within the purposes of transfers under the LED[62].

52. The EDPS welcomes that according to **Article 14(2)(a), the processing of personal data received under the Protocol**[63] **has to be limited to the scope of application of the Protocol**.

53. **As far as subsequent processing of the received data is concerned**[64], the EDPS welcomes the **prohibition set out in Article 14(2) to further process the personal data for an incompatible purpose**[65], **and when it is not permitted under the domestic law of the Party**. In this regard, the EDPS considers positively, the encouragements provided by the explanatory report to the competent authorities to make an overall assessment of the specific circumstances such as *'(i) the relationship between the initial and further purpose (for example any objective link); (ii) the (potential) consequences of the intended further use for the individuals concerned, taking into account the nature of the personal data (for example their sensitivity); (iii) any reasonable expectations of the individuals concerned regarding the purpose of further use and which entities might process the data; and (iv) the manner in which the data will be processed and protected against improper use*'[66].

54. As mentioned above, the subsequent processing of personal data received under this Protocol for a compatible purpose is permitted under the Protocol only in so far as it complies with Article 13 as implemented by each Party in accordance with relevant principles of its domestic law[67].

55. The EDPS further notes that **Article 14(2)(b)** provides that the receiving Party shall ensure under its domestic legal framework that personal data sought and processed are relevant to and not excessive in relation to the purposes of such processing[68].

56. In addition, **Article 14(2)(a)** specifies that '*this article shall not prejudice the ability of the transferring Party*[69] *to impose additional conditions pursuant to this Protocol in a specific case, however, such conditions shall not include generic data protection conditions*'[70], such as requiring that the requesting Party has a specialised data protection authority whereas different systems for oversight are accepted under Article 14[71]. According to the explanatory report[72], such conditions may be imposed to the extent provided for in Chapter II of this Protocol.

57. It is therefore the understanding of the EDPS that, should the receiving authority not be in a position to comply with all or part of these additional conditions, a refusal, prevention or narrowing down as the case may be, in a specific case, of the transferred data, would not fall within this latter prohibition, as it will be grounded in the specific circumstances at hand.

58. As far as the **data transferred as part of the request or order is concerned**, Chapter II of the Protocol contains specific provisions allowing the requesting Party to include in its request or order any special procedural instructions, which includes any request for confidentiality or for non disclosure of the personal data to the registrant, the subscriber or other third parties[73]. It is to be noted, however, that the Protocol only creates an avenue for co-operation but does not impose the obligation to seek assistance on its basis. Hence, should the request for additional safeguards by the requesting authority not be satisfied, the Protocol leaves the possibility to the Parties to use other channels of co-operation otherwise available (Article 5(7)). It is therefore the understanding of the EDPS, that, as far as Member States are concerned, such other co-operation mechanisms could be relied upon provided they comply with EU law.

59. As far as **the requested data** is concerned, the EDPS notes positively that Article 6 contains the obligation to use the requested data only for the specific criminal investigation or proceeding for which the data is requested. Article 7(5)(c)(ii) - which under the Proposal of the Commission would be applicable in the Member States, Articles 8 and 10 of the Protocol allow the requested Party to make the supply of the information or material in response to a request

dependent on the conditions that it is not used for investigations or proceedings other than the one stated in the request[74]. Under Article 9(6) of the Protocol, the requested Party may specify any conditions under which it would provide the data, which could include therefore a limitation or other condition as to its further use, such as being informed of such further processing. The possibility to impose a use limitation on the data received under the Protocol is confirmed by the explanatory report, which further clarifies the exceptions to that possibility[75].

60. Regarding transfers under Article 7, the explanatory report[76] clarifies that the procedure under paragraph 5(d)[77] - '*may also provide an opportunity to clarify aspects of the confidentiality of the information sought as well as any intended use limitation by the authority seeking the data*'.

61. Therefore, while the EDPS regrets that no general mechanism has been foreseen in the Protocol to inform the relevant Member States' competent authorities of a further processing, he notes that the Protocol offers a framework allowing the Party transferring data to impose limitation as to the further use of the data and which could be used by the Parties as well to be kept informed of a further processing should it occur. In this regard, the explanatory report clarifies that '*the material may be used for another purpose where the prior consent of the transferring Party has been obtained*'[78]. Once in force, the Protocol would create a favorable environment for parties as the case may be to bilaterally agree on any further transparency measure, such as handling codes.

### 4.3.2. Storage limitation and data retention principles

62. The Protocol provides in Article 14(5) for an obligation to retain the personal data only for as long as necessary and appropriate in view of the specific purposes in accordance with Article 2 of the Protocol for which the data are processed. The data may therefore be retained for the duration of the investigation and subsequent proceeding and for further processing that is not incompatible with the original purpose. In order to comply with this obligation, Parties have to provide in their domestic legal framework for specified retention periods and/or the review of the need for further retention at planned intervals. According to the explanatory report, Parties '*should ensure in their legal framework that competent authorities develop internal rules and/or procedures for implementing the specific retention periods and/or periodic review of the need for further retention. If the retention period has expired or if the Party has determined through periodic review that there is no further need to retain the data, they should be deleted or rendered anonymous*'[79].

### 4.3.3. Accuracy principle

63. Article 14(3) of the Protocol provides that each Party shall take reasonable steps to ensure that personal data are maintained with such accuracy and completeness and are as up to date as is necessary and appropriate for the lawful processing of the personal data, having regard to the purposes for which they are processed. According to the explanatory report, '*Parties are encouraged to take reasonable steps to ensure that where data provided to or received from another authority are found to be incorrect or outdated, the other authority is informed as soon as practicable in order to make corrections to the extent necessary and appropriate given the purposes of processing*'[80].

### 4.3.4. Security, integrity and confidentiality principles

64. The Protocol raises important questions regarding the security of transferred personal data. The EDPS wishes to stress that ensuring the security of personal data is not only a clear requirement under EU law[81], but it is also considered by the CJEU in relation to the essence of the fundamental right to data protection. Data security is also essential to ensuring the secrecy of investigations and the confidentiality of criminal proceedings.

65. The EDPS therefore welcomes Article 14(7), which imposes on the Parties the obligation to ensure that appropriate technological, physical and organisational measures are in place for the protection of personal data and in case of a security incident '*in which there is a significant risk of physical or non-physical harm to individuals or to the other Party'*, to take promptly appropriate action to mitigate such harm and provides for the notification by the receiving Party of a security incident to the transferring authority and to the data subject.

66. The EDPS also takes positive note of the explanation given in the explanatory report[82].

67. In addition, Chapter II of the Protocol expressly provides that where a request or an order is submitted in electronic form, appropriate level of security and authentication may be required[83].

### 4.3.5. Maintaining records or logging (accountability principle)

68. The EDPS welcomes the obligation pursuant to Article 14(8) of maintaining records or having other appropriate means such as logging[84] to demonstrate how an individual's personal data are accessed, used and disclosed in a specific case. He regrets, however, that this obligation is not more detailed as to what information shall be contained. Also he notes negatively that this obligation is applicable only to certain processing activities (access, use and disclosure) and not to other processing activities such as storage.

### 4.3.6. Sensitive data

69. According to the CJEU case law[85], the need for safeguards applies particularly where the protection of the particular category of personal data that is sensitive data is at stake.

70. With regard to **what constitutes a special category of personal data under the Protocol**, the EDPS notes positively that Article 14(4) of the Protocol includes 'personal data revealing racial or ethnic origin, political opinions or religious or other beliefs, or trade union membership; genetic data and biometric data *considered sensitive in view of the risks involved;* or personal data concerning health or sexual life'[86]. It authorises the processing of such sensitive data only 'under appropriate safeguards to guard against the *risk of unwarranted prejudicial impact from the use of such data*, in particular against unlawful discrimination'[87].

71. It is to be noted that Article 14(2)(b) - to be read in conjunction with Article 13 (see above) - requires specifically to ensure that '*personal data sought and processed are relevant to and not excessive in relation to the purposes of such processing*'[88] and appropriate safeguards have to be in place in case of automated decisions making (Article 14(6) see below).

72. As far as the **processing of the sensitive data is concerned** - be it the data contained in the request or the requested data, it shall be noted that in relation to the principle of security enshrined in the Protocol (see above), the explanatory report encourages parties to design and implement measures that take into account the sensitivity of the data[89]. Besides, in case of

onward sharing within a Party, the data shall be processed in accordance with Article 14 and any onward transfer has to be authorised by the transferring authority (Article 14(9) and (10), see below).

73. For **transferring data in response to a request or an order issued** under the Protocol, a transferring authority may, in a specific case, add conditions as to the use of the data (Article 14(2)(a)) to the extent provided in Chapter II of the Protocol (Measures for enhanced co-operation). Chapter II provides either for a non-binding request with the possibility to provide for conditions under the domestic law - which could therefore be specific conditions linked to the special category of data at stake - on the one hand, or, on the other hand, for the co-operation under Articles 7, 8 and 10, with the possibility either to add specific conditions - which could therefore be linked to the special category of data at stake[90] - or to refuse to transfer the requested data, should the order, despite the safeguards imposed by the Protocol on the order[91], amount to violating the essential interests of the requested Party (Article 27(4) of the Cybercrime Convention) or based on Article 25(4) of the Cybercrime Convention[92].

74. As far as the **data part of the request or order is concerned**, Chapter II of the Protocol contains specific provisions allowing the requesting Party to include in its request or order any special procedural instructions, which includes any request for confidentiality or for non disclosure of the personal data to the registrant, the subscriber or other third parties[93].

75. It is therefore the opinion of the EDPS, that it would be possible for an authority to require in a specific case additional safeguards as to the processing of biometric data in the receiving Party, even if the biometric data is not deemed a sensitive data within the meaning of paragraph 4 by the receiving Party.

### 4.3.7. Automated decisions

76. According to the case law of the CJEU, '*the need for [...] safeguards is all the greater where personal data is subject to automated processing. Those considerations apply particularly where the protection of the particular category of personal data that is sensitive data is at stake*'[94].

77. The EDPS welcomes that Article 14(6) prohibits automated decisions '*based solely on automated processing of personal data*' where they produce *'a significant adverse effect concerning the relevant interests*' of the data subject, unless such decision is *'authorised under domestic law and with appropriate safeguards'*. Such safeguards against a significant adverse effect concerning the relevant interests of the data subject *'include the possibility to obtain human intervention*'. This ensures that no automated decision based on the received data under the Protocol shall take place without the possibility for a human being to intervene and without appropriate safeguards. This is especially important in the area of law enforcement, where the consequences of profiling on individuals are potentially more severe.

78. It is to be noted that the explanatory report mentions that, *'[a]ppropriate safeguards are critical to reducing the potential impact to the relevant interests of the individual to whom the personal data relate*'[95]. It is to be read in conjunction with Article 13 according to which the powers and procedures provided for in this Protocol are subject to conditions and safeguards provided for under the domestic law of each Party, which '*shall provide for the adequate protection of human rights and liberties*'.

79. In addition, with regard to **special categories of personal data** received and processed by a law enforcement authority under the Protocol, the Protocol provides that processing of sensitive data shall only take place under appropriate safeguards to guard '*against the risk of unwarranted*

*prejudicial impact from the use of such data*"[96], in particular against unlawful discrimination (Article 14(6) combined with Article 14(4)).

80. Finally, as mentioned in the above section on purpose limitation and data minimisation, Article 14(2)(b) of the Protocol provides an obligation on the requesting Party to seek and process data that are relevant and not excessive in relation to the purposes of such processing. Furthermore, the Protocol allows the transferring Party to impose conditions as to the subsequent use of the data (Article 14(2)(a) to be combined with Chapter II- Measures of enhanced co-operation - see above). It is therefore the understanding of the EDPS that, for instance, a Member State's transferring authority may in a specific case, impose any specific measure suitable to safeguard the data subject's rights and freedoms and legitimate interests in the specific case at hand. This is therefore all the more important that, Member States avail themselves, as proposed by the Commission, of the declaration provided for under Article 7(5) so that in a requested Member State, an authority is always involved, should the Council decide to authorise them to sign and ratify, in the interest of the Union, the Protocol, without reserving the right not to apply Article 7[97].

### 4.3.8. Onward sharing within a Party

81. The EDPS welcomes the provisions under Article 14(9) related to onward sharing within a Party and notes positively that the processing by the other authority in the receiving Party shall process the received data under the Protocol in accordance with Article 14. The explanatory report[98] clarifies that the procedure under Article 7(5)(d) - which under the proposals of the Commission would be applicable in the Member States (see below) - may also provide an opportunity to clarify aspects of the confidentiality of the information sought, as well as any intended use limitation by the authority seeking the data. In addition, it is possible under Chapter II of the Protocol for the requesting authority to give special instructions for non disclosure of the request to subscribers or other third parties[99].

### 4.3.9. Onward transfer to another State or international organisation

82. The EDPS welcomes the provision under Article 14(10), mandating the prior authorisation of the transferring authority for the transfer by the receiving Party to another State or international organisation.

### 4.3.10. Consultation and suspension

83. The EDPS welcomes that the Protocol provides, under Article 14(15) for a specific provision allowing for the suspension of the transfer to a Party to the Protocol in case of '*systematic or material breach of the terms of [Article 14] or that a material breach is imminent*'.

84. In particular, with regard to the fact that Article 14(1)(d) prohibits further authorisation for transfers, the EDPS would recall that the establishment in the Member States of independent national supervisory authorities is an essential component of the protection of individuals with regard to the processing of their personal data[100]. National supervisory authorities are responsible for monitoring compliance with EU data protection law pursuant to Article 8(3) of the Charter and each authority is vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with data protection law even when the legal system of a third country has been found adequate or a presumption of compliance is introduced on a basis of an agreement.

#### 4.3.11. Review

85. The EDPS welcomes the introduction under Article 23 of a mechanism to periodically assess the effective use and implementation of the provisions of this Protocol and the clarification in the explanatory report[101] that *'[i]n view of the relevant expertise necessary for the assessment of the use and implementation of some of the provisions of this Protocol, including on Article 14 on data protection, Parties may consider involving their subject-matter experts in the assessments*'.

### 4.4. Measures for enhanced co-operation

#### 4.4.1. General remarks

86. The EDPS first would like to recall that, according to Recital 71 of the LED, where transfers by law enforcement competent authorities are not based on a adequacy decision, 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. He therefore welcomes that the co-operation provisions of the Protocol under Articles 7, 8 and 10, by introducing Article 27(4) of the Cybercrime Convention as a ground for a refusal of a transfer, allow a transferring Party to take into account this risk and refuse to transfer data on that basis.

87. In addition, the EDPS understands that **privileges and immunities** may be invoked by a requested Party as a ground for refusal to production orders on a case-by-case basis, on the basis of Articles 25(4) and 27(4) of the Cybercrime Convention[102] or can be added by a Party as part of the reasonable conditions under domestic law for non binding requests under Articles 6 and 9[103].

88. The EDPS finally welcomes that no provision on **direct access to data by law enforcement authorities** has been included in the final text of the Protocol.

#### 4.4.2. Disclosure of subscriber information by service providers directly to competent authorities of another Party (Article 7)

##### 4.4.2.1. Limitation to the status of requesting authorities by the requested Party

89. The EDPS welcomes that the Annex instructs the Member States to make the declaration pursuant to Article 7(2)(b), indicating that orders submitted to service providers in their territory must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision.

##### 4.4.2.2. Systematic involvement of a judicial authority in the requested Party

90. The EDPS welcomes the instruction given to the Member States in the Annex to notify, pursuant to Article 7(5)(a) of the Protocol, that when an order is issued under Article 7(1), to a service provider in their territory, simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation or proceeding to their authorities is required. Such authorities have the powers to instruct the service provider not to disclose the subscriber information if:

    i. disclosure may prejudice criminal investigations or proceedings in that Party; or

ii. conditions or grounds for refusal would apply under Article 25(4), and Article 27(4), of the Cybercrime Convention[104] had the subscriber information been sought through mutual assistance.

91. In this regard, pursuant to Article 7(5)(e), Parties shall designate a single authority to receive such notification. However, neither the Article nor the Annex specifically mention the type of authority. Given that the competent authority ordering the disclosure of the information might not be a judicial or other independent authority[105], the EDPS **recommends instructing Member States to designate a judicial or other independent authority to receive the notification** in order to give these authorities the possibility to effectively review compliance of the orders with the Cybercrime Convention and perform the actions described in paragraph 5, points b, c and d. Such involvement would also be more in line with Article 82(1) TFEU.

92. In this regard, the EDPS recalls that in its case law, concerning access to communications data for law enforcement purposes, the **CJEU has subjected the possibility to provide for such access, among other criteria, and '*except in cases of validly established urgency*'[106], to a '*prior review carried out by a court or an independent administrative body*'**, '*following a reasoned request by [competent national] authorities submitted, inter alia, within the framework of procedures for the prevention, detection or criminal prosecution*'[107]. The systematic involvement of judicial authorities in the requested Parties is also essential to preserve the application of the principle of dual criminality[108] in the field of judicial co-operation as it would allow for an adequate and appropriate authority to verify such circumstances leading to the application of this principle. The EDPS recalls that the dual criminality principle aims at providing an additional safeguard to ensure that a State cannot rely on the assistance of another to apply a criminal sanction which does not exist in the law of another State.

#### 4.4.2.3. Definitions and types of data

93. The EDPS notices that the definition of subscriber information, as per Article 18(3) of the Cybercrime Convention, may also include information that under EU law constitutes traffic data. Namely, information needed for the purpose of identifying a subscriber of a service may indeed include certain Internet Protocol (IP) address information – for example, the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time, which under EU law constitute traffic data relating to the transmission of a communication[109].

94. In addition, in accordance with the relevant CJEU case law, to establish the existence of an interference with the fundamental right to privacy, it is not relevant whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way. The CJEU has furthermore ruled in its judgment in joined cases C-203/15 and C-698/15 Tele2 Sverige AB that metadata such as traffic data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications[110].

95. Given that the balance between the types of offences for which an order can be issued and the categories of data concerned should be assessed in order to limit the possibility to submit an order to produce data that could be considered as traffic data which access is justified by the fight against serious crimes only, **the EDPS recommends Member States to reserve the right not to apply Article 7 in relation to certain types of access numbers, pursuant to Article 7(9)(b), contrary to the instruction of the Commission in the Annex** in order to ensure a more substantial involvement of the authorities of the requested State. He notes in

this regard that the Protocol provides for an alternative avenue for expedited production of data under Article 8 between competent authorities of the Parties concerned.

#### 4.4.3. Giving effect to orders from another party for expedited production of subscriber information and traffic data (Article 8)

96. The EDPS welcomes the instruction given by the Commission to Member States to declare under Article 8(4), that additional supporting information is required to give effect to orders under Article 8(1), which will depend on the circumstances of the order and the related investigation or proceeding; this being particularly important in order for the authorities to be able to make an adequate decision in accordance with Article 8(8) of the Protocol.

97. The EDPS notes in addition that the Commission instructs '*Member States that participate in the enhanced co-operation established by Regulation (EU) 2017/1939 implementing enhanced co-operation on the establishment of the European Public Prosecutor's Office ('the EPPO') [to] include the EPPO, in the exercise of its competences as provided for by Articles 22, 23 and 25 of Regulation (EU) 2017/1939, among the authorities communicated under Article 8, paragraph 10, point a and point b*' i.e. among the authorities designated to submit or receive an order for expedited production of subscriber information and traffic data.

98. The EDPS reiterates that, according to the CJEU case law, the CJEU has restricted the possibility to provide for such access, among other criteria, and 'except in cases of validly established urgency'[111], to a 'prior review carried out by a court or an independent administrative body' (see paragraph 92 above). Therefore, he underlines that a prosecutor of a Member State and consequently the EPPO should be able to submit an order or transfer data based on the order of another Party under this provision only where a review by a judicial authority or an independent body within the meaning of the CJEU case law is ensured[112].

# 5. On enforceable data subject rights and effective legal remedies for data subjects.

## 5.1. The right to information, the right of access, the right of rectification and erasure

99. The EDPS recalls that the right of access and the right to rectification are essential elements of the right to data protection under Article 8(2) of the Charter. If the exercise of data subjects' rights are usually limited in the law enforcement context in order to avoid jeopardising ongoing investigations, the possibility for data subjects to exercise their rights should exist in practice and not remain purely theoretical, even if limited or exercised through an authority in situations where the exercise of these rights is denied to protect sensitive law enforcement information.

100. The Protocol includes provisions on the right to be informed (Article 14(11)), the right of access (Article 14(12)(a)(i)) and the right to rectification - which also refers to erasure and blocking (Article 14(12)(a)(ii)) and the right not to be subject to automated decisions (Article 14(6) - see above).

101. The **right to information** is of utmost importance as it allows the exercise of other data protection rights, including the right to remedies, and ensures fair processing of the data[113].

Data subjects usually have no knowledge of the fact that their data are processed (or transferred) for law enforcement purposes. The EDPS recalls that in the context of transfers by private entities, in its Opinion 1/15, the CJEU found that '*air passengers must be notified of the transfer of their PNR data to Canada and of its use as soon as that information is no longer liable to jeopardise the investigations being carried out by the government authorities*' considering that *'[t]hat information is, in fact, necessary to enable the air passengers to exercise their rights to request access to PNR data concerning them and, if appropriate, rectification of that data, and, in accordance with the first paragraph of Article 47 of the Charter, to an effective remedy before a tribunal*'[114].

102. The EDPS welcomes therefore the inclusion under Article 14(11) of an obligation on each Party to provide notice with regard to the processing, through the publication of general notices, or through personal notice to the data subject. While it can be regretted that such obligation does not include the obligation to provide for the contact details of the controller, the EDPS notes that the Protocol imposes the obligation to provide notice with regard to the legal basis for and the purpose(s) of processing, any retention or review periods as applicable, access, rectification and redress available and recipients or categories of recipients to whom such data are disclosed.

103. The right to information applies also in case of onward sharing, in relation to the subsequent processing of the data by an authority (Article 14(9)).

104. The Protocol ensures moreover the individual notice of the data subject where the law of the transferring party provides for it. If the other Party has requested that the provision of data be kept confidential where the conditions for the restrictions under the Protocol apply, such individual notice shall take place only once the restrictions no longer apply[115]. Individual notice may be restricted under the same conditions as the right of access (see below).

105. The **right of access and the right to rectification** are essential elements of the right to data protection under Article 8(2) of the Charter. Furthermore, as regards Article 7 of the Charter, the Court has held that '*the fundamental right to respect for private life, enshrined in that article, means that the person concerned may be certain that his personal data are processed in a correct and lawful manner. In order to carry out the necessary checks, that person must have a right of access to the data relating to him which is being processed*'[116].

106. The EDPS welcomes therefore the inclusion under Article 14(12) **of a right of access and rectification, which includes the right to erasure.**

107. The Protocol provides that the right of access may be subject to restrictions (point (a)). The EDPS recognises that the exercise of data subjects' rights is usually limited in the law enforcement context in order to avoid jeopardising ongoing investigations. In this regard, the EDPS considers positively that the Protocol expressly provides that the restrictions shall be proportionate and necessary to protect the rights and freedoms of others or important objectives of general public interest and give due regard to the legitimate interests of the data subjects. He regrets, however, that the Protocol does not require the domestic legal framework of the Parties to make sure that the possibility for data subjects to have access to their own data, de facto, exists, even if limited or exercised through an authority.

108. The EDPS regrets that the Protocol allows the imposition of a fee for obtaining access (point (b)). However he notes that it shall be limited to what is reasonable and not excessive 'given the resources involved' 'in order not to dissuade or discourage access' according to the explanatory report[117]. It is also the understanding of the EDPS that such fee may not be imposed for exercising the right of rectification, including the right for erasure.

## 5.2. Judicial redress and administrative remedies

109. The EDPS recalls that, in the different context of an adequacy finding decision (the Safe Harbor), the CJEU found[118] that the lack of effective judicial redress when personal data are transferred to a third country goes to the essence of Article 47 of the Charter, which provides for the right to an effective judicial protection. In that context, the CJEU found that '*legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter*" and that "*the first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to* ***an effective remedy*** *before a tribunal in compliance with the conditions laid down in that article*'[119].

110. Also, the CJEU has stressed that it is essential for individuals to be able to file complaints with independent supervisory authorities[120] and seek, therefore, administrative redress.

111. The EDPS therefore welcomes that Article 14(13) provides that each Party shall have in place an effective judicial and non judicial remedies to provide redress for violations of this Article.

## 5.3. Oversight: control by an independent authority

112. Article 16 TFEU and Article 8(3) of the Charter include as essential guarantee of the right to data protection the control by an independent authority. While each Member State has appointed an independent authority in charge of supervising the data processing activities, including the transfer of data to third countries, there is also a need for an effective independent oversight once the data have been transferred in the receiving third countries.

113. The EDPS recalls that, pursuant to the CJEU case law[121], an independent supervisory authority within the meaning of Article 8(3) of the Charter is an authority able to make decisions independently from any direct or indirect external influence. Such a supervisory authority must not only be independent from the parties it supervises, but it should also not be '*subordinate to a further supervisory authority, from which it may receive instructions*' as this would imply that it is '*not free from any external influence liable to have an effect on its decisions*'[122].

114. The EDPS welcomes Article 14(14) on oversight, which requires from each Party to have in place an oversight authority, independent and which details the effective powers that this specific authority or authorities may exercise over authorities to which personal data would be transferred on the basis of the Protocol. It stems from the explanatory report that *'[t]he authorities should perform their tasks and exercise their powers impartially; they should enjoy the ability to act free from external influence that could interfere with the independent exercise of their powers and functions; in particular such authorities should not be subject to instructions, in a particular case, as to the exercise of their investigation powers and/or the taking of corrective action; and, finally, it is important that the authorities have the necessary skills, knowledge and expertise to perform their duties, and receive appropriate financial, technical and human resources for the effective performance of their functions*'[123]. The EDPS emphasises that, should it be ascertained in practice that another Party would not provide for an independent oversight authority essentially equivalent to the EU standards, Member States should be allowed to avail themselves of the suspension provision in case of a systematic or material breach of this Article 14, under Article 14(15).

115. While no specific co-operation mechanism between the respective oversight authorities is provided by the Protocol and Parties are not required to notify their oversight authority, the EDPS notes positively that Parties are encouraged in the explanatory report to promote co-operation between their respective oversight authorities. '*Consultations between the Parties' respective authorities when carrying out their oversight functions under this article may take place as appropriate. This may include the exchange of information and best practices*'[124].

# 6. Relationship between the data protection provision (Article 14) of the Protocol and other agreements

116. In view of the multilateral character of the Protocol, Article 14(1)(b) and (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.

## 6.1. Relationship between the EU and the United States of America

117. While the safeguards of Article 14, paragraphs 2 to 15 apply by default to Parties receiving personal data, on the basis of Article 14(1)(b), *'[i]f, at the time of receipt of personal data under this Protocol, both the transferring Party and the receiving Party are mutually bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data which is applicable to the transfer of personal data for the purpose of the prevention, detection, investigation and prosecution of criminal offences, and which provides that the processing of personal data under that agreement complies with the requirements of the data protection legislation of the Parties concerned, the terms of such agreement shall apply, for the measures falling within the scope of such agreement, to personal data received under the Protocol in lieu of paragraphs 2 to 15, unless otherwise agreed between the Parties concerned'.*

118. The EDPS notes that, according to the explanatory report[125], an example of such agreement is the EU-U.S. Umbrella Agreement[126] and that '*the terms of such agreements shall apply in lieu of paragraphs 2 to 15 for the measures falling within the scope of such agreements*'.

119. The EDPS welcomes in this regard that the Commission proposes to the Member States to communicate to the authorities of the United States of America the understanding of the EU in this regard.

120. The EDPS understands that it is confirmed that the Umbrella Agreement would apply to transfers from the EU to the United States of America in the framework of the provisions set out in the Protocol related to the **co-operation between authorities.** The EDPS regrets such outcome.

121. As far as **direct co-operation provisions of the Protocol are concerned** (Articles 6 and 7), the EDPS would like to recall that the Umbrella Agreement would not be applicable[127]. For it to be the case, it would need to be modified by an agreement between the EU and the United States, which shall contain additional safeguards. He refers in this respect to his Opinion on the Commission Recommendation for a Council Decision authorising the opening of negotiations to conclude an international agreement with the United States of America on cross-border access to electronic evidence[128]. Therefore, it is the understanding of the EDPS that, until such agreement is adopted and entered into force between both Parties, the safeguards contained in Article 14 of the Protocol would apply to the processing of personal data received by a Party under the direct co-operation provisions of the Protocol.

122. The EDPS understands that the communication proposed by the Commission aims at further clarifying that for the direct co-operation provided for under the Protocol, the Umbrella Agreement would not apply between the EU and the US in lieu of paragraphs 2 to 15 of Article 14 of the Protocol. It stems indeed from Article 14(1)(b) of the Protocol read in conjunction with the requirements set out in EU law that, only a legally binding instrument concluded between the EU and the United States in the form of an international agreement, amending the Umbrella Agreement and providing for the necessary additional safeguards, could meet the conditions set out in Article 14(1)(b) of the Protocol for its provisions on data protection to apply in lieu of paragraphs 2 to 15 of Article 14 of the Protocol. The EDPS **would therefore recommend, should the Council decide to authorise Member States to sign and ratify the Protocol, clarifying even further the proposed communication, which currently refers to "specific transfer arrangement".**

## 6.2. Relationship between the EU and other third country Parties to the Protocol

123. Article 14(1)(c) of the Protocol provides that '*[i]f the transferring Party and the receiving Party are not mutually bound under an agreement described in paragraph 1.b, they may mutually determine that the transfer of personal data under this Protocol may take place on the basis of other agreements or arrangements between the Parties concerned in lieu of paragraphs 2 to 15*'[129].

124. The EDPS **welcomes the Commission's intention**, in its consideration, to clarify that Member States are bound by the EU law framework as it stems from Chapter V of the GDPR and the LED, when determining whether they could avail themselves of the provisions of Article 14(1)(c) of the Protocol to apply other data protection provisions agreed between the Parties on transfers of personal data under the Protocol, in lieu of paragraphs 2 to 15 of Article 14 of the Protocol.

125. The EDPS would however **recommend clarifying further this consideration, should the Council decide to authorise Member States to sign and ratify the Protocol**.

126. In particular, he would like to highlight that the said agreements should meet the conditions set out in Chapter V of both the GDPR **and** the LED.

127. The consideration refers inter alia to an '*agreement or arrangement [which] ensures appropriate data protection safeguards pursuant to Article 46 of the General Data Protection Regulation*'.

128. The EDPS would like to further underline that one important objective of the Protocol has been to provide appropriate data protection safeguards in a legally binding international agreement to services providers in the EU when transferring data upon request by third country authorities. Given that the Protocol refers to 'agreements or arrangements between the Parties concerned', the EDPS therefore would like to invite the Commission to explain which agreements or arrangements may provide for appropriate data protection safeguards pursuant to Article 46 of the GDPR for transfers from service providers or entities providing domain name registration services located in the EU to authorities of a third country Party to the Protocol.

# 7. Conclusions

129. Considering the proliferation of cybercrime and the increasing importance of electronic evidence for criminal investigations, in view of the complexity of obtaining such evidence when it is not within the Member States jurisdiction, the EDPS understands the need for law enforcement authorities to obtain electronic evidence quickly and effectively to ensure they can effectively fight crime.

130. The EDPS is therefore in favour of finding an international response with appropriate safeguards to existing issues in this context.

131. The Protocol aims both at improving the traditional co-operation channels and at providing for direct co-operation between law enforcement authorities and service providers cross-border. It does not contain provisions on direct access to data by law enforcement authorities, which the EDPS welcomes.

132. While recognising that it is not possible to replicate entirely the terminology and definitions of EU law in a multilateral international agreement, the EDPS underlines that appropriate data protection safeguards for individuals must be ensured in order to fully comply with EU law.

133. The EDPS is satisfied that the Protocol contains a dedicated Article on the protection of personal data. He also notes positively the many safeguards that have been included in the Protocol.

134. The EDPS understands that it is confirmed that the Umbrella Agreement would apply to transfers from the EU to the United States of America in the framework of the provisions set out in the Protocol related to the co-operation between authorities. The EDPS regrets such outcome.

135. Should a Council Decision be adopted authorising the Member States to, respectively sign and ratify, in the interest of the Union, the Protocol, the EDPS welcomes the proposals of the Commission for the Member States to make, in the interest of the Union, the declaration, notification and communication under Article 7(2)(b), (5)(a) and (e) of the Protocol. These proposals ensure that service providers in the Union may be requested the transfer of personal data only on the basis of orders issued in the requesting third country Party to the Protocol by, or under the supervision of, a prosecutor or other judicial authority, or under independent supervision and under the control of a competent authority within the requested Member State.

136. He also notes positively the proposal that Member States make the declaration under Article 8(4) of the Protocol (on the co-operation between competent authorities to give effect to production orders of subscriber information and traffic data), so as to ensure that additional supporting information is required to give effect to orders under this provision.

137. The EDPS has the following recommendations in relation to the future Council Decisions, should the Protocol be signed and ratified by the Member States, in the interest of the Union:

- Certain data contained within the category of subscriber information within the meaning of the Cybercrime Convention, may be deemed under EU law as traffic data entailing a serious interference with the fundamental rights of the data subject, access to which may be justified only by the fight against serious crime. Therefore, the EDPS recommends Member States, contrary to the Proposals of the Commission, to reserve the right not to

apply Article 7 of the Protocol on disclosure of subscriber information by service providers directly to competent authorities of another country in relation to certain types of access numbers, pursuant to Article 7(9)(b);

- Member States should designate, pursuant to Article 7(5)(e) of the Protocol, a judicial or other independent authority;

- The proposed communication by the Member States to the United States authorities, at the time of signature or when depositing their instrument of ratification, acceptance or approval, in relation to the EU-US Umbrella Agreement should be clarified;

- The proposed consideration in relation to other agreements or arrangements under Article 14(1)(c) of the Protocol that could replace the data protection provision of the Protocol (Article 14) should be amended.

138. The EDPS finally underlines that a prosecutor of a Member State and therefore also the EPPO should be able to submit an order or transfer data based on the order of another Party under Article 8 only where it is ascertained that such order is subject to a review by a judicial authority or an independent body within the meaning of the case law of the CJEU.

139. The EDPS remains at the disposal of the Commission, the Council and the European Parliament to provide further advice during the process. This Opinion is without prejudice to any additional comments that the EDPS could make on the basis of further available information.

Brussels, 20 January 2022

*[e-signed]*
Wojciech Rafał WIEWIÓROWSKI

# Notes

[1] OJ L 119, 4.5.2016, p. 1.
[2] OJ L 295, 21.11.2018, p. 39.
[3] OJ L 119, 4.5.2016, p. 89.
[4] https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690
[5] Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), COM(2019) 71 final.
[6] https://rm.coe.int/1680a49dab (provisional version as approved by the Committee of Ministers).
[7] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561
[8] EDPS Opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention of 2 April 2019.
[9] Council Decision adopted on 6 June 2019 authorising the European Commission to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185).
[10] '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'
[11] European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade.
[12] Article 21 of the Protocol.
[13] Recital 10 of the Proposals for a Council Decision authorising Member States to sign and ratify, 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.
[14] 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 (COM(2021)718 final).
Proposal for a Council Decision authorising Member States to ratify, 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 (COM(2021)719 final).
According to Recitals 14 and 15 of the Proposal on signature and Recitals 13 and 14 of the Proposal on the ratification, Ireland has the option to take part in the adoption and application of the Decision and Denmark is not taking part in the adoption of this Decision and is not bound by it or subject to its application.
[15] Recital 3 of the Proposals.
[16] Article 16(1). '[...][Parties to the Convention] may express their consent to be bound by either:
a. signature without reservation as to ratification, acceptance or approval; or
b. signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval'.
2. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
[17] All except Ireland, which has signed but not ratified the Convention, but nevertheless committed to pursuing accession.
[18] 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/-/conventions/treaty/185/signatures?p_auth=ZZawh58m
[19] See Articles 23-35 of the Cybercrime Convention.
[20] https://rm.coe.int/1680a49c9d as noted by the Committee of Ministers on 17 November 2021.
[21] See par. 2 of the explanatory report to the Protocol.
[22] Within the meaning of the Cybercrime Convention, Article 18(3), 'the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
a the type of communication service used, the technical provisions taken thereto and the period of service;
b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement'.
[23] Within the meaning of the Cybercrime Convention, "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of

communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.
[24] Within the meaning of the Cybercrime Convention, "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
[25] Paragraph 172 of the explanatory report: "Because Article 10 of this Protocol is limited to the emergencies justifying such rapidly expedited action, it is distinct from Article 25, paragraph 3, of the Convention, in which requests for mutual assistance may be made by expedited means of communications in urgent circumstances that do not rise to the level of emergency as defined. In other words, Article 25, paragraph 3, is broader in scope than Article 10 of this Protocol, in that it covers situations not covered in Article 10, such as ongoing but non-imminent risks to life or safety of persons, potential destruction of evidence that may result from delay, a rapidly approaching trial date, or other types of urgencies. While the mechanism in Article 25, paragraph 3, provides for a more rapid method of conveying and responding to a request, the obligations in the case of an emergency under Article 10 of this Protocol are significantly greater; that is, where there is significant and imminent risk to life or safety of a natural person, the process should be even more accelerated (see paragraph 42 of this explanatory report for examples of emergency situations)."
[26] Par. 77 and 169 of the explanatory report.
[27] 'A Party that reserves to this article is not permitted to issue orders under paragraph 1 to service providers in other Parties' territories', explanatory report, par. 122 and 123.
[28] 'A Party that reserves to this article is not permitted to issue orders for traffic data to other Parties under paragraph 1', explanatory report, par. 147.
[29] Annex, section 1.
[30] Annex, sections 2 et 3.
[31] EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, 10 July 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en .
[32] Case C-181/73, R. & V. Haegeman v. Belgian State, ECLI:EU:C:1974:41, par. 5.
[33] Case C-308/06, Intertanko and Others, ECLI:EU:C:2008:312, par. 42.
[34] Joined cases C-402/05 P and C-415/05 P, Kadi v. Council, ECLI:EU:C:2008:461, par. 285.
[35] Either as part of the Member States' requests and orders or in response to such requests and orders.
[36] In response to a request or an order under Articles 6 and 7 of the Protocol.
[37] Par. 99 of the explanatory report clarifies that in 'Article 7, the term "a service provider in the territory of another Party" requires that the service provider be physically present in the other Party. Under this article, the mere fact that, for example, a service provider has established a contractual relationship with a company in a Party, but the service provider itself is not physically present in that Party, would not constitute the service provider being "in the territory" of that Party. Paragraph 1 requires, in addition, that the data be in the service provider's possession or control'. See also par. 77 of the explanatory report in respect of Article 6.
[38] 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.
[39] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1.
[40] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592.
[41] ibid., par. 214.
[42] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 95.
[43] See par. 76 of the explanatory report: 'The objective of Article 6 is to provide an effective and efficient framework to obtain information for identifying or contacting the registrant of a domain name. The form of implementation depends on the Parties' respective legal and policy considerations. This article is intended to complement current and future internet governance policies and practices'.
[44] Par.100.
[45] See for instance albeit, in absence of an international agreement, EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, 10 July 2019.
[46] Article 6(2) of the Protocol and par. 82 of the explanatory report; Article 7(1) of the Protocol and par. 100 of the explanatory report.
[47] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108 (hereinafter 'Convention 108').

[48] See in this regard, Art. 29 WP Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime, of 22 March 2001 (5001/01/EN/ Final WP 41), p. 6: 'signatories should be requested to sign up to the Council of Europe's Convention 108'. It appears in particular that not all third countries parties to the Cybercrime Convention are parties to the Convention 108 or to the European Convention of Human Rights and that some are parties to the African Union Convention on Cyber Security and Personal Data Protection. The protocol amending the Convention 108 so called Convention 108 + has not yet entered into force. It has been signed by 26 Member States and ratified by 11 Member States - see the chart of signature and ratification of the convention 108+: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures
[49] Andorra, Argentina, Canada, Israel, Japan, the United Kingdom and Switzerland.
[50] Par. 220 of the explanatory report.
[51] Without prejudice to the conditions and grounds of refusal available for the requested Party (see below).
[52] Emphasis added.
[53] According to Article 15 of the Cybercrime Convention, '[e]ach Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental
Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and **which shall incorporate the principle of proportionality**.
2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties' (emphasis added).
[54] Par. 231 of the explanatory report.
[55] Emphasis added.
[56] See Article 2 in section 4.3.1.
[57] See par. 97 of the explanatory report. This stems also from Articles 7(1), 8(1) and 9(1), which use the term "specified" information.
[58] See for instance in this regard:
- Article 6(3)(c), Articles 7(1) and 8(1) referring to the need of the information and the explanatory report, in particular par. 82, 84 and 97.
- Article 8, par. 129 of the explanatory report, which clarifies that the mechanism used to compel the service provider to provide the information will be subject to the terms of the law of the requested Party, since the requested Party's procedures will control it. 'Therefore, the requested Party can ensure that its own law, including constitutional and human rights requirements, is satisfied, especially in relation to any additional safeguards including those necessary for the production of traffic data'.
[59] Reasonable conditions of the domestic law of the requested Party under Article 6(2) and any conditions under Article 9(6), which provide in any event for not binding requests (see also par. 77, 82 and 169 of the explanatory report to the Protocol). In addition, under Article 8(7), the requested Party may specify any conditions under which it could comply with the request. See also under Articles 8(8) and 10(7) of the Protocol the condition stemming from Article 28(2)(b) of the Cybercrime Convention (condition not to use the information for investigations or proceedings other than those stated in the request) and under Articles 7(5)(c)(ii), 8(8) and 10 of the Protocol (see par. 173 of the explanatory report), conditions stemming from Article 25(4) of the Cybercrime Convention according to which the assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties.
[60] Par. 269 of the explanatory report to the Cybercrime Convention clarifies that under Article 27(4) of the Convention, 'refusal of assistance on data protection grounds may be invoked only in exceptional cases. Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting Party would raise difficulties so fundamental as to be considered by the requested Party to fall within the essential interests ground of refusal. A broad, categorical, or systematic application of data protection principles to refuse co-operation is therefore precluded. Thus, the fact the Parties concerned have different systems of protecting the privacy of data (such as that the requesting Party does not have the equivalent of a specialised data protection authority) or have different means of protecting personal data (such as that the requesting Party uses means other than the process of deletion to protect the privacy or the accuracy of the personal data received by law enforcement authorities), do not as such constitute grounds for refusal. Before invoking "essential interests" as a basis for refusing co-operation, the requested Party should instead attempt to place conditions which would allow the transfer of the data' (emphasis added). Such ground of refusal is available under:

- Article 7(5)(c)(ii) (direct co-operation with service providers for the production of subscriber information), provided that the requested Party had availed itself of the possibility to require the consultation of its authority - which the Commission proposes for Member States in Annex;

- Article 8(8) (co-operation between authorities for the expedited production of subscriber information and traffic data);
- Article 10(7) (emergency mutual assistance).

See in addition the grounds of refusal under Articles 7(5)(c)(ii), 8(8) and 10 of the Protocol (see par. 173 of the explanatory report), stemming from Article 25(4) of the Cybercrime Convention according to which the assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation.

[61] Emphasis added.

[62] As to the principle of proportionality, see section 4.2.

[63] Par. 221 of the explanatory report clarifies that 'each Party shall process personal data that it receives under this Protocol in accordance with the specific safeguards set out in paragraphs 2 to 15. This includes personal data transferred as part of an order or request under this Protocol.'

[64] For onward sharing and onward transfers, see below.

[65] See as well as the detailed explanations in the explanatory report on what could constitute a purpose, which is not incompatible, under par. 227 and onwards.

[66] Par. 228. 'The legal framework of a Party may further set out particular limitations regarding other purposes for which the data may be used'.

[67] Article 13 and explanatory report, par. 218.

[68] See above on the interpretation of 'relevant and not excessive'.

[69] According to Article 3(1)(e) of the Protocol, '"transferring Party" means the Party transmitting the data in response to a request or as part of a joint investigation team or, for the purposes of Chapter II, section 2, a Party in whose territory a transmitting service provider or entity providing domain name registration services is located'.

[70] Emphasis added.

[71] Explanatory report, par. 230.

[72] Par. 230.

[73] Articles 6(3)(d), 7(4)(f), 8(3) and 9(3)(g), par. 84, 105, 106, 131, 135 and 165 of the explanatory report as well as Article 10(7) combined with Article 27(3) of the Cybercrime Convention.

[74] Articles 6(3)(c), 8(8) and 10(7).

[75] See par. 71.

[76] Par. 111.

[77] According to Article 7(5)(d), the notified authorities of the requested State may request, for the purposes of instructing the service provider not to disclose the subscriber information, additional information from the authority in the requesting Party to which the service provider shall return the subscriber information or otherwise response, and shall not disclose the received additional information to the service provider without that authority's consent. It shall also promptly inform the same authority if the service provider has been instructed not to disclose the subscriber information and give the reasons for doing so.

[78] Par. 71.

[79] Par. 241 and 242.

[80] Par. 234.

[81] Article 5(1)(f) GDPR and Article 4(1)(f) LED.

[82] Par. 246-247.

[83] Articles 6(4), 7(6), 8(5), 9(4) and 10(2) and par. 86, 116 and 174 of the explanatory report.

[84] Par. 258.

[85] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 141.

[86] Emphasis added.

[87] Emphasis added.

[88] This is to be read together with the purpose limitation principle embedded in Chapter II and Article 13 as far as the information requested is concerned: see in particular section 4.2. on the principle of proportionality and section 4.3.1. on the purpose limitation and data minimisation above.

[89] Par. 248.

[90] See footnote 59.

[91] See sections on principle of proportionality, and purpose limitation and data minimisation above.

[92] See sections on principle of proportionality and purpose limitation and data minimisation, in particular footnote 60.

[93] Articles 6(3)(d), 7(4)(f), 8(3) and 9(3)(g), par. 84, 105, 106, 131, 135 and 165 of the explanatory report as well as Article 10(7) combined with Article 27(3) of the Cybercrime Convention.

[94] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par.141.

[95] Par. 245.

[96] See above section 4.3.6.
[97] See below.
[98] Par. 111.
[99] Articles 6(3)(d), 7(4)(f), 8(3) and 9(3)(g), par. 84, 105, 106, 131, 135 and 165 of the explanatory report as well as Article 10(7) combined with Article 27(3) of the Cybercrime Convention.
[100] See Case C-518/07, Commission v Germany, EU:C:2010:125, par. 25; Case C-288/12, Commission v Hungary, EU:C:2014:237, par 48.
[101] Par. 322.
[102] Articles 7(5)(c)(ii), 8(8) and 10(7).
[103] Articles 6(2) and 9(6).
[104] Article 25 General principles relating to mutual assistance - par. 4: 'Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence'. Offences referred to in Articles 2 to 11 of the Convention are a list of offences against the confidentiality, integrity and availability of computer data and systems, computer and content related offences, offences related to infringements of copyright and related rights, aiding or abetting the commission of these offences and the attempt of committing certain other offences established in the Convention.
Article 27- Procedures pertaining to mutual assistance requests in the absence of applicable international agreements- par. 4: 'The requested Party may, in addition to the grounds for refusal established in Article 25,paragraph 4, refuse assistance if:
a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
b it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.'
[105] According to Article 3(2)(b) of the Protocol, '"competent authority" means a judicial, administrative or other law-enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings'.
[106] Joined cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970, par. 120.
[107] Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd, ECLI:EU:C:2014:238, par. 62.
[108] Article 5(6) of the Protocol and par. 69 of the explanatory report.
[109] Par. 93 of the explanatory report to the Protocol.
[110] Joined cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970, par. 99.
[111] Joined cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970, par. 120.
[112] Case C-746/18, Prokuratuur ECLI:EU:C:2021:152, operative part of the judgment: '2.Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation that confers upon the public prosecutor's office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation'.
[113] Case C-201/14, Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Naţională deAsigurări de Sănătate, Agenţia Naţională de Administrare Fiscală, ECLI:EU:C:2015:638, par. 33: 'the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed [...], and their right to object to the processing of those data [...]'.
[114] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 220 [emphasis added].
[115] Article 14(11)(c) of the Protocol.
[116] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 219.
[117] Explanatory report, par. 276.
[118] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 95.
[119] ibid. par. 95 [emphasis added].
[120] ibid. par. 56 to 58.
[121] Case C-518/07, Commission v Germany, ECLI:EU:C:2010:125, par. 25; Case C-614/10, Commission v Austria, ECLI:EU:C:2012:631, par. 36 and 37; Case C-288/12, Commission v Hungary, par. 48.
[122] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 229 and 230.
[123] Par. 278 and onwards.
[124] Par. 281.

[125] Par. 222.
[126] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, OJ L 336, 10.12.2016, p. 3 (hereinafter "the Umbrella Agreement"). The Umbrella Agreement entered into force on 1 February 2017 and establishes a framework for the protection of personal data exchanged between the EU and the US for law enforcement purposes.
[127] See EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection.
[128] EDPS Opinion 7/2019 on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters.
[129] Emphasis added.