

Letters



Mr Juan Fernando López Aguilar
Chairman
Committee on Civil Liberties, Justice and Home Affairs
European Parliament

Sent by email only

Brussels, 22 February 2022
Ref: OUT2022-0008

Dear Mr López Aguilar,

Thank you very much for your letter of 15 November 2021 on behalf of the Committee on Civil Liberties, Justice and Home Affairs (the Committee), in which you inform about the Committee's request for an EDPB opinion on the final draft of the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (the Protocol).

The EDPB welcomes your request and the opportunity to recall its views for the Committee. The EDPB had indeed already called on the European Commission and European Parliament, as well as on EU Member States and national parliaments, to ensure that the Protocol negotiations receive careful scrutiny in order to guarantee the full consistency of the envisaged Second Additional Protocol with the EU acquis, in particular in the field of personal data protection.

In this context, the EDPB had the occasion to provide and publish its observations and recommendations during the negotiating process of the Protocol, addressing its points of concern and attention in relation to the draft provisions published at the time, and in particular in its latest contribution (annexed to this letter) to the 6th round of consultations in May 2021 on the draft Protocol, which has been since then adopted by the Committee of Ministers of the Council of Europe on 17 November 2021.

In response to your Committee's request, the EDPB wishes to recall some of the aspects of earlier statements and in the light of the two Commission's Proposals for Council Decisions authorising Member States to sign and to ratify, in the interest of the European Union, the Protocol (the Proposals). The EDPB regrets to note that many of its recommendations to the negotiations on the draft of the Protocol, to a great extent, are not reflected in the final version of the text.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Additionally, the EDPB wishes to refer to the EDPS Opinion 1/2022 on the above-mentioned Proposals. The EDPB wishes to highlight and complement some of the crucial points identified by the EDPS. Furthermore, the EDPB encourages the Committee to consider and address the EDPS Opinion and its recommendations in its assessment of the Protocol.

On the effect of the Protocol and the Proposals

The Council of Europe Convention on Cybercrime (hereinafter Cybercrime Convention), as well as any of its additional protocols, are to be considered as a legally binding and enforceable international instrument. In this regard, the EDPB stresses that, in line with the CJEU case law, 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.”¹

The EDPB reiterates that from the perspective of the European Union and its Member States the Protocol must be assessed in light of EU law and case law, in particular by considering the provisions on appropriate safeguards as referred to in Chapter V of Regulation (EU) No 2016/679 (GDPR) and Chapter V of Directive (EU) No 2016/680 (Law Enforcement Directive) and their interpretation by the Court of Justice of the European Union (CJEU) in light of the EU Charter.

In this context, the EDPB emphasizes that Article 44 of the GDPR lays down provisions to ensure that any transfer of personal data from EU Member States to third countries shall only take place if the level of protection guaranteed by the GDPR is not undermined. Where the transfer is conducted by a competent authority as defined in Article 2(1) Law Enforcement Directive, the equivalent is specified by Article 37 of that Directive. Given that the Protocol could have an effect on the application of these provisions of EU law in the context of transfers, the EDPB reiterates that several provisions of the Protocol, and in particular those under Chapter II, section 2 related to the direct cooperation with providers and entities in other Parties may, given the level of norm and legal effect of the Protocol, also have an effect on transfer and disclosure, as per Chapter V GDPR and in particular its Article 48. It is therefore essential that the level of protection resulting from the Protocol for the exchange of personal data with third countries is essentially equivalent to the level of protection provided by EU law.²

On measures for enhanced cooperation

The EDPB 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

¹ CJEU Judgment of 3 September 2008 in joined cases C-402/05 P and C-415/05, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, ECLI:EU:C:2008:461, par. 285.

² See also EDPS Opinion, paragraph 32.

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.³

The EDPB 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.⁴

In order to ensure the involvement of independent authorities, the EDPB fully supports the EDPS recommendation⁵ for Member States to designate, pursuant to Article 7(5)(e) of the Protocol, a judicial or other independent authority.

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 (e. g. dynamically allocated addresses in IPv4) and the access to such data may entail a serious interference with the fundamental rights of the data subject. The CJEU has held in its recent case-law⁶ that, access of national authorities to retained traffic data may be justified only by the fight against serious crime, and subject to a prior review carried out either by a court or by an independent administrative body. Therefore, the EDPB recommends, in line with the EDPS Opinion,⁷ that Member States, contrary to the proposal of the Commission, 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).

Finally, in relation to measures for enhanced cooperation, the EDPB reiterates the essential nature of the dual criminality principle, which 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. In this regard, while the EDPB notes the lack of explicit reference to dual criminality in the Protocol other than in Article 5(6), the EDPB understands that this permission is to be found where the Protocol allows parties to add conditions to or refuse the transfer under their domestic law.⁸

On the conditions and safeguards related to the protection of personal data

While taking note of the further clarifications provided in the Explanatory Report,⁹ the EDPB regrets that the extent to which parties may add further conditions and safeguards to the transfer of personal

³ See also EDPS Opinion, paragraphs 89 and 90.

⁴ See also EDPS Opinion, paragraph 96.

⁵ EDPS Opinion, paragraphs 91 and 92.

⁶ C-511/18 - La Quadrature du Net and Others of 6 October 2020.

⁷ EDPS Opinion, paragraphs 93-95.

⁸ See also paragraph 69 of the Explanatory Report.

⁹ Explanatory Report, Paragraph 230.

data and the extent to which they may not be added, if they are considered as generic data protection conditions pursuant to Article 14(2)(a), have not been made clearer.¹⁰

In relation to the application of the proportionality principle and in line with its previous contribution (page 6), while welcoming the direct reference to Article 15 of the Cybercrime Convention in the Protocol,¹¹ the EDPB regrets that the application and implementation of the principle of proportionality is not explicitly included in the text of Article 13, in order to ensure legal certainty and clarity, and to enshrine this principle for any processing of personal data resulting from the application of the Protocol.

The EDPB regrets that its proposal concerning the onward sharing within a party to establish a mechanism to inform the transferring party of an envisioned onward sharing and further processing has not been implemented.¹²

The reference to the Parties' domestic legal framework in Paragraph 11 of Article 14 of the Protocol, read in conjunction with paragraph 12(a)(i) of Article 14, implies that possible limitations and restrictions to transparency and notice are to be permitted under the domestic legal framework of the receiving Party. The EDPB acknowledges, in line with the EDPS Opinion, that paragraph 12(a)(i) of Article 14 of the Protocol imposes specific conditions for such laws, as it provides for the "*application of proportionate restrictions permitted under [the receiving Party's] domestic legal framework, needed, at the time of adjudication, to protect the rights and freedoms of others or important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned*". The EDPB wishes to recall in this regard that the domestic legal framework of third country Parties to the Cybercrime Convention applicable to restrictions on transparency and notice may significantly diverge from the ones in the Union or Member States' law, thus possibly resulting in limitations that may not be considered as compatible with Union or Member States' law.

The EDPB also regrets that its recommendations in relation to the exercise of data subject rights have not been taken into account and in particular that the provision under paragraph 12(b) does not ensure that, as a general rule, information to individuals related to access shall be provided free of charge.

While welcoming the obligation under the Protocol that "[e]ach Party shall have in place effective judicial and non-judicial remedies to provide redress for violations of *this article*" (paragraph 13 of Article 14), the EDPB regrets that neither the text of the Protocol nor the explanatory report explicitly clarifies that such redresses are available under the jurisdiction of each Party to the Cybercrime Convention to any concerned data subjects, as per the EDPB recommendation made in its previous contribution (page 12). Such application is essential to ensure full compatibility with EU law and

¹⁰ See also in this regard EDPS Opinion, paragraphs 46, 56-60, 75, 80, 81 and 86- 87.

¹¹ See also paragraph 218 of the Explanatory Report.

¹² See also EDPS Opinion, paragraph 61.

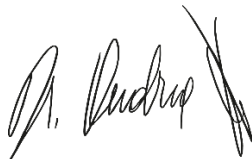
appears all the more important considering that not all Parties to the Cybercrime Convention fall under the jurisdiction of the European Court of Human Rights.

The EDPB welcomes the provisions on oversight and recommends (in line with the encouragement in the Explanatory Report¹³) establishing mechanisms to foresee the cooperation and exchange of information between established public authorities ensuring oversight in each Party, thus allowing for a coordinated and consistent supervision of the implementation of the Protocol and contributing to the assessment foreseen under its Article 23. In addition, the EDPB would like to emphasise that, in agreement with the EDPS Opinion, it considers that an eventual lack of an independent supervisory authority in another Party would constitute a systematic and serious breach within the meaning of paragraph 15, thus allowing transfers to be suspended to that Party.

In addition, with regard to the Council decisions, and in line with the EDPS Opinion,¹⁴ 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 in the Council's decisions, in line with the EDPS Opinion.¹⁵

Yours sincerely,



Andrea Jelinek

¹³ Explanatory Report, paragraph 281. See also EDPS Opinion, paragraph 115.

¹⁴ EDPS Opinion, paragraphs 121-122.

¹⁵ EDPS Opinion, paragraphs 123-128.