Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention

Why is the opinion of the Court of Justice of the European Union necessary?

Executive summary

European Digital Rights (EDRi) is a network of 45 organisations from across Europe. We promote and defend rights and freedoms in the digital environment.

EDRi calls on the European Parliament to use its power under Article 218(11) of the Treaty of the Functioning of the EU (TFEU) to request the opinion of the Court of Justice of the EU (CJEU) on the compatibility of the Second Additional Protocol (hereafter the Protocol) **of the Council of Europe (CoE) Cybercrime Convention with the Treaties, including the Charter of Fundamental Rights.**

The compatibility of the Second Additional Protocol with EU law is unclear. Civil society raised these concerns during the process and propose modifications and improvements of the text to avoid these risks. However, those modifications and improvements were not incorporated into the final text. As Member States of the EU will be considering adherence to this Protocol, it is important to ensure that this text is in line with EU law prior to ratification. A judgment of the CJEU delivered after the Protocol has been ratified and determining that one or more provisions of the Protocol are incompatible with the Treaties, would inevitably provoke serious difficulties for the EU internally and for the EU's international cooperation with third countries. If the Protocol as such were to be deemed to be incompatible with the Treaties prior to ratification, it might need to be amended before EU Member States can ratify the Protocol. While EDRi's own analysis leads to this conclusion, as outlined below, it is also possible that the application of the Protocol to the EU Member States and the EU itself can be made compatible with EU law through reservations and declarations that Article 19 of the Protocol expressly provides for. These reservations and declarations must however be made at the time of ratification. Only a prior opinion of the CJEU can ensure that Member States make the appropriate choices when implementing the Protocol.

We also wish to highlight that, as an international agreement, the Protocol will be superior to EU secondary law such as the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), and hence may undermine important safeguards in these instruments. An opinion of the CJEU will provide legal guidance on this issue which is crucial in order to ensure that any decision of the Parliament on whether or not to give its consent to the agreement under TFEU Article 218(6) is duly considered and informed.

In this paper, we point out the shortcomings of this international agreement in terms of fundamental rights protections which, if ratified by EU Member States without further amendments (or at least significant reservations and declarations), could lead to substantive breaches of EU law. The paper focuses on the direct transfers of personal data from service providers in the EU to law enforcement authorities in third countries (Articles 6 and 7), and is not exhaustive for the potential incompatibility of the Protocol with the Treaties.

Our analysis, which takes into consideration the opinions of the European Data Protection Supervisor (EDPS) and Board (EDPB), points out the following issues in particular:

- The possibility to refuse direct requests is too limited;
- The review by a court or independent administrative authority is not guaranteed; and
- Specific measures ensuring compliance with the essential equivalence requirements are missing

The possibility to refuse direct requests is too limited

For direct requests to service providers, involvement of authorities in the requested State with the possibility to refuse requests is critical for protecting fundamental rights and other safeguards in Member States' criminal procedure law, e.g privileges, immunities and special protections accorded to certain people such as lawyers, journalists and whistleblowers. This is possible, in principle, if Member States require simultaneous notification of their authorities for all production orders under Article 7, by making a notification to this effect under Article 7(5)(a) of the Protocol. Article 7(5)(c)(ii) provides for the same grounds for refusal as for mutual legal assistance treaties (MLAT) requests for subscriber information under the Budapest Convention [Article 25(4) and Article 27(4)].

Under the draft Council Decision [COM(2021) 719 final], Member States would be obliged to make this notification to other Parties of the Protocol. However, **notification is, in itself, not sufficient to safeguard fundamental rights of individuals in the EU. Member States must also ensure that the notification has suspensive effects on the order**, so that service providers are not allowed to respond before authorities in the requested Member State have considered relevant grounds for refusal and made a decision about whether to refuse or uphold the order.

Articles 6 on direct requests to domain name registration services has no specific provisions for notification of authorities in the requested State. Therefore, there is no avenue for assessing and applying grounds for refusal in this case. Unlike Article 7, requests under Article 6 are in principle voluntary (non-binding) for service providers, but delegating the responsibility for protecting fundamental rights to private service providers is not an acceptable principle under EU law. In footnote 59 to his Opinion, the EDPS refers to Article 6(2), which says that the response of service providers can be subject to "reasonable conditions provided by domestic law", as a possibility to refuse requests under Article 6. However, **it is unclear how Article 6(2) can ensure the involvement of authorities in the requested State and allow them to order providers to refuse certain requests**, especially without placing a considerable burden on private companies which do not have the capacity, the mandate or the inherent interest to review each request for possible violations of fundamental rights or safeguards in criminal procedure law.

Review by a court or independent administrative authority is not guaranteed

The CJEU has held consistently that law enforcement authorities' access to personal data stored by private companies must be made subject to prior review by a court or an independent administrative authority, except in cases of validly established urgency.[i] **The Protocol does not ensure this, as requests under Article 6 and orders under Article 7 are issued in accordance with the domestic law of the requesting Party.**

(1) Article 7

The draft Council Decision requires Member States to make the declaration under Article 7(2)(b) that orders under Article 7(1) must be "issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision." This is not sufficient to ensure compatibility with CJEU case law as a prosecutor is not recognised as an independent judicial authority.[ii]

As proposed by the EDPS, prior authorisation by a court or independent administrative authority can be achieved under Article 7, if Member States designate a court or an independent administrative authority to receive notifications and scrutinise every order [Article 7(5)(e)] before they are executed by service providers.

Considering that certain Member States where large service providers are established may receive a large number of production orders, **EDRi considers it highly unlikely that these Member States would opt for mandatory notification to domestic courts with suspensive effects unless an opinion from the CJEU instructs them to do so in order to ensure compatibility with the Charter.**

Such an opinion could also add crucial specific requirements as to the possible nature and status and guarantees of actual independence of any authority other than a judicial one. Without such guidance, Member States may establish authorities that do not meet the relevant EU law requirements – which would then have to be established in lengthy and costly litigation.

(2) Article 6

For requests under Article 6, the Protocol does not allow a Party to make a declaration about which authorities can issue such requests, and no involvement of authorities (let alone courts) in the requested State is foreseen.

In light of the CJEU case law about prior court authorisation, **this deficiency makes it unlikely that Article 6 is compatible with the Charter.** Only an opinion from the CJEU before ratification can clarify this (and other) critical aspects of the Protocol.

The risk not to meet the Court's requirements for essential equivalence is considerable

We identify three main areas of doubt as regards the Protocol's compatibility with the CJEU's requirement of essential equivalence in relation to cross-border data transfers (*in casu*, the provision of data from the EU to third countries). The Court has introduced very strict requirements to prevent an undermining of the level of protection of individuals' rights when their data are transferred outside the EU in three cases: *Schrems I, Opinion 1/15, and Schrems II*.[iii]

(1) Absence of measures permitting the assessment of third countries' domestic law, international commitments and practice

The Protocol is meant to provide a legal basis for transfers of personal data to other State Parties, either between law enforcement authorities or from private service providers to law enforcement authorities. Article 14(1)(d) obliges Parties to ensure that requirements in their personal data protection legal framework for such personal data transfers to other Parties are satisfied, and that transfers may only be refused for reasons of data protection under the conditions set out in Article 14(15). Parties to the Protocol must adhere to the data protection provisions in Article 14 when processing personal data received under the Protocol. In lieu of Article 14, paragraphs 2-15, Parties may use an international agreement establishing a comprehensive data protection framework between parties.

From the viewpoint of EU law, the Protocol must establish appropriate safeguards when personal data are transferred from the EU by either law enforcement authorities (LED, Article 37) or private service providers (GDPR, Article 46) to any Party to the Protocol.

Yet, the Cybercrime Convention and the Protocol are open to accession by States outside the Council of Europe area (subject to invitation), which do not necessarily have robust data protection frameworks. Even some of the current Parties to the Cybercrime Convention do not have domestic data protection laws and are not parties to Convention 108/108+ of the Council of Europe. Furthermore, unlike adequacy decisions, no individual assessment of the legal framework of third-country Parties is foreseen, as the Protocol, and in particular Article 14, is assumed to provide appropriate safeguards for the transfer.

For Standard Contractual Clauses, the data exporter in the EU has an obligation to assess the legal framework of the third country to which personal data are transferred, and to assess whether, in spite of the clauses, "supplementary measures" may be required to protect the data against undue access by the authorities in the receiving country (including its secret services)[iv], as established by the CJEU in *Schrems II*. The draft Council Decision does not designate an entity in the EU with a similar obligation to monitor and assess the domestic legal framework of third countries to which personal data can be transferred from the EU under the Protocol.

In practice, DPAs will have considerable difficulties in assessing whether or not a potentially large number of third countries comply with Article 14 when receiving personal data under the Protocol. The Protocol does not envisage international cooperation between Parties' data protection authorities, and some Parties may not even have dedicated (and independent) DPAs.

EDRi considers this systemic lack of accountability and assessment mechanisms for ensuring compliance with the Charter the main deficiency of the Protocol.

Considering the high risk that safeguards provided for by the Protocol to ensure essential equivalence for transfers may be compromised under the legal framework of some Parties, it is therefore essential to obtain the opinion of the CJEU on whether the Protocol as such is compatible with EU law.

(2) Further processing of personal data received under the Protocol

The limits imposed on further processing of personal data in the requesting State are not sufficiently specified, and therefore are unlikely to satisfy the Court's case law.

In its *Opinion 1/15*, the CJEU found that some provisions for further processing in the envisaged EU-Canada Passenger Name Record (PNR) agreement were "too vague and general to meet the requirements as to clarity and precision required".[v]

Article 14(2)(a) of the Protocol provides that personal data should not be further processed for an incompatible purpose. However, the Explanatory Report (ER) gives a very broad description of what constitutes a not incompatible purpose. Paragraph 229 of the ER provides **a very extensive and non-exhaustive, vague list of not incompatible purposes, that is unlikely to withstand CJEU scrutiny. Therefore, the current text is unlikely to satisfy the Court's criteria of essential equivalence.**

Some provisions of the Protocol permit the imposition of more specific use limitations for personal data. In such cases, further processing generally requires the consent of the transferring Party, which may to some extent remedy the vague definition of not incompatible purposes, although a formal consent and notification scheme is not foreseen in the Protocol, as noted by the EDPS. However, Article 7 has no provisions that directly allow for use limitations. The EDPS refers to Article 7(5)(c)(ii) in this regard, which allows for the application of conditions or grounds for refusals under Articles 25(4) and 27(4) of the Cybercrime Convention had the subscriber information been sought through mutual legal assistance. However, we consider this option more limited and certainly less clear for the requested State than e.g. Article 8(8) that explicitly refers to the possibility to impose use limitations in addition to conditions or grounds for refusal under Articles 25(4) and 27(4) of the Cybercrime Convention.[vi]

As a result, only an opinion of the CJEU can help clarify whether the Protocol allows Member States to restrict further processing to be compatible with EU law and requirements of essential equivalence, including to what extent use limitations can be invoked for that purpose,

in particular when personal data are transferred directly from private service providers (Article 7).

(3) Data subjects' rights

Another major weakness of the Protocol is that compliance with data subjects rights, including ensuring that restrictions are limited to what is strictly necessary, is left entirely to the domestic laws of the Party to which personal data are transferred. We believe that domestic laws of some Parties manifestly fail to meet the requirements for essential equivalence with EU law. The CJEU specified in paragraph 95 of *Schrems I* that legislation not providing for any possibility for individuals to pursue legal remedies in order to have access to their own personal data would be contrary to the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. Enforceable data subject rights must moreover exist in practice, not just on paper. The EDPS seems to recognise this in paragraph 107 of his Opinion.

In our opinion, the Protocol fails to ensure that the right to effective judicial protection as enshrined in the Charter will be provided, in particular by non-European State Parties.

(4) Suspension of transfers

Even though Article 14(15) provides the possibility to suspend transfers to a third country, there are too many obstacles to activate this system. The requirement of "systematic or material breach" sets a high bar for suspending transfers compared to other transfers based on appropriate safeguards, e.g. standard contractual clauses in *Schrems II*. Moreover, the main rule in Article 14(15) is that transfers can only be suspended after consultation with the other Party, which in the context of an international agreement takes place at the government level. The Protocol does not provide for a cooperation mechanism between independent DPAs. **This undermines the independence of EU Member States' DPAs as they cannot suspend transfers without involving and obtaining the agreement of the government of their Member State.**

Given the many concerns raised by civil society organisations and the European Data Protection Board and Supervisor, we recommend to the European Parliament to request an opinion of the CJEU in order to inquire the compatibility of the Protocol with EU law.

Background

The European Parliament is required to give its consent to the approval of the Commission's proposal for Council decisions authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. Under Article 218(11) of the Treaty of the Functioning of the EU (TFEU), the European Parliament may obtain the opinion of the Court of Justice of the EU (CJEU) as to whether an envisaged international agreement is compatible with the Treaties. Where the opinion of the Court is adverse, the envisaged agreement envisaged may not enter into force unless it is amended or the Treaties are revised.

European Digital Rights (EDRi) has been sending submissions to the Council of Europe (CoE) since 2016 and took part in all consultation rounds organised by the leading Cybercrime Committee to ask for human rights to be respected.[vii] It joined the Octopus conferences organised by the CoE and the roundtables organised by the European Commission on the developments of the negotiations.

i For example, in the Tele2/Watson case the CJEU ruled that "it is essential that access of the competent national authorities to retained data should, as a general rule, be subject to a prior review carried out by a court or independent administrative body, except in cases of validly established urgency." http://curia.europa.eu/juris/liste.jsf?num=C-203/15

ii Prokuratuur C-746/18, paragraph 59 https://curia.europa.eu/juris/liste.jsf?num=C-746/18

iii *Schrems I*, https://curia.europa.eu/juris/liste.jsf?num=C-362/14
Opinion 1/15, https://curia.europa.eu/juris/document/document.jsf?docid=193216&doclang=EN
Schrems II, https://curia.europa.eu/juris/liste.jsf?num=C-311/18

iv We use the term "undue access" here as shorthand for access under rules that do not meet the conditions set out in the EDPB's European Essential Guarantees for surveillance (EEGs)

v Paragraph 181: the Court considers that the wording "to ensure the oversight or accountability of the public administration" and "to comply with the subpoena or warrant issued, or an order made, by a court" is too vague to define properly the specific cases in which a third country (in this case, Canada) would be able to further process data received under an international agreement.

vi See Explanatory Report, paragraph 141.

vii Consultation of our submissions can be done following this link: https://edri.org/our-work/cross-border-access-to-data-for-law-enforcement-document-pool/#recommendations