EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)

Brussels, 13th November 2019

Preliminary remarks and context of the EDPB contribution

The European Data Protection Board (EDPB) very much welcomes the opportunity of the consultation held by the Council of Europe Cybercrime Convention Committee (T-CY) on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention). Such consultation process is even more essential considering that the meetings dedicated to the preparation of the additional protocol are being held in closed sessions and that the direct involvement of data protection authorities in the drafting process has not been foreseen in the T-CY Terms of Reference[1]. The EDPB therefore wishes to provide a constructive and objective contribution with a view to ensure that data protection consideration are duly taken into account in the overall drafting process of the additional protocol.

Access to personal data across jurisdictions has already been addressed in the past by EU data protection authorities in various positions and opinions and the EDPB wishes to recall in particular the Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime[2], as well

[1] Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, Approved by the 17th Plenary of the T-CY on 8 June 2017, T-CY (2017)3: https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b

[2] Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime, 05/12/2013: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf

as its statement on data protection and privacy aspects of cross-border access to electronic evidence[3]. The European Data Protection Supervisor issued Opinion 03/2019 on the mandate for the participation of the Commission in the negotiations[4], as well as Opinion 7/2019 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters[5]. This contribution also builds upon the EDPB Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters[6].

The EDPB acknowledges that situations where judicial and law enforcement authorities are faced with a "cross-border situation" with regards to access to personal data as part of their investigations can be a challenging reality and recognises the legitimate objective of enhancing international cooperation on cybercrime and access to information. In parallel, the EDPB recalls that the protection of personal data and legal certainty must be guaranteed, thus contributing to the objective of establishing sustainable arrangements for the sharing of personal data with third countries for law enforcement purposes, which are fully compatible with the EU Treaties and the Charter of Fundamental Rights. The EDPB furthermore shares the objective of enshrining the preparation of the additional protocol within the framework of the Council of Europe core values and principles, and in particular human rights and the rule of law.

With regards to trans-border direct access to stored computer data as per Article 32(b) of the Budapest Convention, the EDPB reaffirms in particular that data controller can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required.

As the Cybercrime Convention, as well as any of its additional protocols, is to be considered as a binding international instrument, 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[7]." It is therefore essential that EU negotiating parties ensure that the provisions laid down in the additional protocol do comply with the EU *acquis* in the field of data protection in order to ensure its compatibility with EU primary and secondary law.

---

[3] WP29 statement on data protection and privacy aspects of cross-border access to electronic evidence, 29 November 2017: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610177

[4] EDPS opinion 3/19 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention: https://edps.europa.eu/data-protection/our-work/publications/opinions/budapest-cybercrime-convention_en

[5] EDPS opinion 7/19 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters: https://edps.europa.eu/data-protection/our-work/publications/opinions/electronic-evidence-criminal-matters_en

[6] Opinion 23/2018 of the EDPB adopted on 26 September 2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters: https://edpb.europa.eu/our-work-tools/our-documents/opinia-art-70/opinion-232018-commission-proposals-european-production_en

[7] See CJEU joined cases C-402/05 P and C-415/05 P, Kadi v. Council, ECLI:EU:C:2008:461 - par (285).

Considering the timeframe of the consultation process, this EDPB contribution will focus on a preliminary assessment of the provisional texts published on 1st October and in particular the new provisions on direct disclosure of subscriber information and on the giving effect to orders from another Party for expedited production of data. The EDPB understands that dedicated provisions on the protection of personal data are still being discussed and will, in this regard, lay down a series of initial recommendations to be considered by the T-CY. As for previous provisions, the EDPB remains available for further contributions and calls for an early and more proactive involvement of data protection authorities in the preparation of these specific provisions, in order to ensure an optimal understanding and consideration of data protections safeguards.

Provisional text of provisions on direct disclosure of subscriber information and on the giving effect of orders for expedited production of data

The EDPB particularly welcomes the opportunity to comment on the draft procedure that provides for the direct cooperation between the authorities of one Party and a service provider in the territory of another Party to obtain subscriber information, as well as on the ability for the requested party to give effect to received order by compelling a service provider in its territory to produce subscriber information or traffic data in the service provider's possession or control. While such provisions may appear of a mainly procedural nature, they are essential in determining the conditions for access to personal data and therefore in assessing a possible interference with the right to the protection of personal data as guaranteed by Article 7 of the Charter of Fundamental Rights of the Union. On the basis of its preliminary assessment, the EDPB recommends further examining the draft provisions with regard to the following elements.

Systematic involvement of judicial authorities of the requested party

The EDPB welcomes the possibility, as per Article 4(5), for a Party to require that an order issued to a service provider in its territory is simultaneously notified to its authorities and that the designated authority may instruct the service provider not to disclose the information if conditions or grounds for refusal would apply under Articles 25.4 and 27.4 of the Convention. However, such safeguard remains at the discretion of each Party to the Convention. As far as EU Parties are concerned, the EDPB stresses that safeguards and limitations affecting the procedural conditions for access to personal data will have to be applied consistently in order to ensure a harmonised level of protection for all persons in the Union.

Article 4(5) does not specifically mention to which type of authority in the requested State orders are to be notified and possibly reviewed. The EDPB recommends that further requirements are included in order to ensure that judicial authorities designated by the authorities of the service provider are involved as early as possible in the process of gathering subscriber information in order to give these authorities the possibility to effectively review compliance of the orders with the Convention and ensure the obligation for these authorities

to raise grounds for refusal on that basis. In this regard, the EDPB recalls that in its case law concerning access to communications data for law enforcement purposes, the CJEU has restricted the possibility to provide for such access, among other criteria, and "except in cases of validly established urgency"[8], to a "prior review carried out by a court or an independent administrative body", "following a reasoned request of [competent national] authorities submitted within the framework of procedures of prevention, detection or criminal prosecution."[9]

The systematic involvement of judicial authorities in the requested parties is also essential to preserve the application of the principle of dual criminality in the field of judicial cooperation. The EDPB 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.

Limitation to the status of requesting authority

The EDPB notes and welcomes that, according to Article 4, paragraph 2b, only the requested Party, via a declaration, can impose that the requesting authority is a prosecutor, a judicial authority or another independent authority. However, this could imply, *a contrario* and in the absence of such declaration, that where the requested State did not make such a declaration, orders to service providers could be issued by any authority in the requesting Party. Due to the direct effect of the additional protocol to the Convention in the EU legal order, the draft provisions could then be interpreted as allowing any authority to issue an order, thus putting the lawfulness of the agreement into question in light of EU law. In light of the CJEU case law already cited, the EDPB considers that the type of requesting authorities who may issue such order should be limited to prosecutor, a judicial authority or another independent authority.

Categories of data, definition of "subscriber information" and type of offence

The EDPB recommends that the definition of subscriber information, as per Article 18.3 of the Convention, be further clarified in order to avoid inclusion of any traffic data or content data. 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. In addition, the EDPB recalls that, in accordance with the relevant CJEU case law, to establish the existence of an interference with the fundamental right to privacy, it does not matter 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 judgement in joined cases C-203/15 and C-698/15 Tele2 Sverige AB that metadata such as traffic data and location 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[10].

[8] See CJEU joint cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970 – par (120)
[9] See CJEU joint cases C-293/12 and C-594/12, Digital Rights Ireland Ltd, ECLI:EU:C:2014:238 – par (62)
[10] See CJEU joint cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970 – par (99)

The EDPB also takes the view that the balance between the types of offences for which an Order can be issued and the categories of data concerned shall be reassessed in order to limit the possibility to submit an Order to produce data that could be considered as traffic data, to serious crimes only. Furthermore, the definition of a common list of specific serious criminal offences should be further explored.

Security of data processing

Although Article 4(6) and Article 5(5) provide that appropriate levels of security and authentication may be required, the EDPB encourages the development of further specifications and requirements in this regard. Ensuring that the necessary means are put in place so that the personal data are disclosed and communicated in a secure environment with the means to ensure the authenticity of documents is key for achieving the objective of a swift gathering of electronic evidence in compliance with fundamental rights.

In relation to the security of data processing, the EDPB also invites the T-CY to consider, as a specific data protection safeguard, a mechanism for the notification without delay of data breaches that could seriously interfere with the rights and freedoms of data subjects. Personal data breaches could indeed potentially have a range of significant adverse effects for individuals concerned.

Provisions on data protection safeguards

The EDPB considers essential that the provisional text submitted to public consultation is complemented by dedicated provisions on data protection safeguards, which must then be assessed together in order to ensure the draft additional protocol translates into a sustainable arrangement for the sharing of personal data with third countries for law enforcement purposes, fully compatible with the EU Treaties and the Charter of Fundamental Rights.

Provisional text of provisions on direct disclosure of subscriber information and on the giving effect to orders from another Party for expedited production of data, by laying down procedural conditions for access to personal data, may already impact on the level of protection of personal data and may also need to be amended in order to ensure the operational application of appropriate data protection safeguards.

The EDPB considers that specific provisions on data protection safeguards shall reflect key principles and in particular lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. These principles are also in line with the Council of Europe modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), to which many Parties to the Convention on Cybercrime are also Party.

Substantive and procedural conditions for access to personal data

As stated by the Article 29 Working Party on data protection and privacy aspects of cross-border access to electronic evidence, the EDPB recalls that the current EU legal framework and the most recent case law can allow the development of a list of substantive and

procedural conditions to be taken into account for any future instrument governing law enforcement access to personal data. Considering the direct effect of an additional protocol to the Convention in the EU legal order, the following conditions for access to personal data remain relevant:

- The conditions under which the providers of electronic communications services must grant such access must be provided by law, so as to ensure that the processing relies on a clear legal basis.
- Individual access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime.
- Access of the competent national authorities to data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body.
- In particular situations, where for example national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.
- Personal data collected should be adequate, relevant and not excessive for the purpose of the processing.
- The processing of special categories of personal data should be subject to further limitations and safeguards.
- The competent national authorities to whom access to the data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardize the investigations being undertaken by those authorities.
- Personal data should be correct, up to date and should not be kept longer than necessary.
- Notification is necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy and their data protection rights in relation to the processing of their data.

Availability of effective legal remedies

The EDPB also considers of paramount importance that the additional protocol includes mechanism to ensure the availability of legal remedies to the data subject whose data has been obtained, at least equivalent to those available in a domestic case. In this regard, the EDPB recalls that the CJEU has stated 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. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law"[11].

[11] See CJEU C-362/14, Maximillian Schrems, ECLI:EU:C:2015:650 – par (95)

Further processing and onward transfer

The EDPB highlights that published provisional texts do not contain any specific limit with regard to the further processing and onward transfers of the transferred personal data by the requesting Party authority. The EDPB therefore recommends specifying narrowly the purposes of the transfers and the prohibition of further processing incompatible with those purposes and including the general principle of prohibition of onward transfers unless the third country provides an appropriate level of protection, in order to prevent the level of protection provided for in the protocol from being circumvented by further processing and onward transfers of personal data to other third countries.

Oversight and monitoring mechanism

In light of the comments and recommendations above, the EDPB finally invites the T-CY to consider the development of a mechanism for the oversight and monitoring by an independent authority, with both investigatory and corrective enforcement powers, responsible to ensure the application of future data protection safeguards in practice.

The EDPB reiterates the importance of involving data protection authorities in the drafting process of the additional protocol and stands ready to contribute and assist the T-CY in the preparation of provisional text of provisions on data protection safeguards.