Statement

# Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)

## Adopted on 2 February 2021

**The European Data Protection Board has adopted the following statement:**

**Preliminary remarks and context of the EDPB statement**

The European Data Protection Board (EDPB) and data protection authorities within the EU are following closely the development of the second additional protocol to the Budapest Convention and have regularly contributed to the consultation held by the Council of Europe, such as the annual « Octopus conference ». In November 2019, the EDPB also published its latest contribution to the consultation on a draft second additional protocol[1], indicating that it remained « *available for further contributions* » and called 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* »[2].

Following up on the publication of new draft provisions of the second additional protocol to the Budapest Convention[3], the EDPB therefore, once again, wishes to provide an expert and constructive contribution with a view to ensure that data protection considerations are duly taken into account in the overall drafting process of the additional protocol, 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[4].

[1] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf
[2] The EDPB upholds the positions and recommendations expressed in this previous contribution and considers relevant to restate key principles in light of the latest developments and new draft provisions published.
[3] https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-convention-on-cybercrime-additional-stakeholder-consultations
[4] 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.

The EDPB furthermore considers that the abovementioned provisions are likely to affect the substantive and procedural conditions for access to personal data in the EU, including as a result of requests from third country authorities, thus also resonating with ongoing debates at EU level and related legislative initiatives currently being considered by the co-legislators[5]. The EDPB therefore calls on the European Commission and European Parliament, as well as on EU Member States and national Parliaments, to ensure that the ongoing 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.

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 yet again 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 another jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime[6], as well as its statement on data protection and privacy aspects of cross-border access to electronic evidence[7]. The European Data Protection Supervisor has issued Opinion 03/2019 on the mandate for the participation of the Commission in the negotiations[8], as well as Opinion 7/2019 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters[9]. These contributions also build upon the EDPB Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters[10].

The EDPB remains fully aware 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 reiterates 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 of the EU. The EDPB furthermore considers it essential to frame 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 a data controller can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need

[5] In particular, but not exclusively, the discussions on the Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters.

[6] 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.

[7] WP29 statement on data protection and privacy aspects of cross-border access to electronic evidence, 29 November 2017.

[8] EDPS opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention.

[9] EDPS opinion 7/2019 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters.

[10] 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.

to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to its domestic law that will specify the purpose for which the data is required.

Since the Budapest Convention, as well as any of its additional protocols, are binding international instruments, 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"[11]. 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.

Considering the timeframe of the consultation process, this EDPB contribution will focus on a preliminary assessment of the new draft provisions of the second additional protocol to the Budapest Convention which have not been subject to previous stakeholder consultations:

- Joint investigation teams and joint investigations
- Expedited disclosure of stored computer data in an emergency
- Request for domain name registration information

Once again, the EDPB understands that dedicated provisions on the protection of personal data are still being discussed. 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 draft provisions on joint investigation teams and joint investigations (JITs) (Article 3), on the request for domain name registration information (Article 6) and on expedited disclosure of stored computer data in an emergency (Article 7)**

On the basis of its preliminary assessment, the EDPB recommends further examining the provisional draft provisions with regard to the following elements.

The EDPB notes that both the requests for domain name registration information and for expedited disclosure of stored computer data in emergency cases are non-binding requests and grounds for refusal to comply with the request are not clearly defined, while the possibility to rely on the law of the requested State Party to refuse such cooperation, including grounds for refusal set out in MLATs, is also unclear[12]. The EDPB recalls in this regard that the conditions under which the providers of electronic communications services or the entity providing domain name services must grant such access must be provided by law, so as to ensure that the processing relies on a clear legal basis.

[11] See CJEU joined cases C-402/05 P and C-415/05 P, Kadi v. Council, ECLI:EU:C:2008:461 - par (285).
[12] The draft Article 6 (2) refers to "reasonable conditions provided by domestic law" for instance.

The EDPB additionally refers to its previous contribution to reinstate that, except in cases of validly established urgency[13] and, in light of the CJEU case law[14], the EDPB considers that the type of requesting authorities who may issue such request should be limited to a prosecutor, a judicial authority or another independent authority. The EDPB also considers that the systematic involvement of judicial authorities in the requested parties is essential to ensure an effective compliance review of the requests with the Convention and to preserve the application of the principle of double criminality in the field of judicial cooperation.

The EDPB recalls in this regard that the double criminality principle aims at providing an additional safeguard to ensure that a Party cannot rely on the assistance of another to apply a criminal sanction, which does not exist in the law of this other Party. In addition to ensuring respect of individuals' rights and due process in the envisioned mechanism of judicial cooperation, such safeguard also provides for an essential guarantee related to the procedural conditions for access to their personal data. As already mentioned in its previous contribution, in relation to the security of data processing, the EDPB 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.

In relation to the provisional draft provisions on the request for domain name registration information, the EDPB stresses that such information includes personal data and that therefore any international instrument laying down substantive and procedural conditions for accessing such data must, for the Parties members of the European Union, be compliant with EU primary and secondary law.

In relation to the provisional draft provisions on "expedited disclosure of stored computer data in an emergency" (Article 7), the EDPB notes that, depending on its application by each party, this new provision may involve the direct disclosure of content data. The EDPB also notes that the requested State Party may require, after the disclosure of the data, that a proper mutual assistance request is provided (Article 7(5)). In this latter case however, there is no commitment by the Parties to the envisaged Protocol, to delete the data or not to use it as evidence if, on the basis of the supplementary information obtained in the proper mutual assistance request, the requested authorities conclude that the conditions were not met to disclose the data. The legal consequences for the disclosed data, once in the requesting country, seem therefore to be completely left to the discretion of that country's national law. The lack of commitment at the level of the protocol therefore entails the risk to strip this provision of any protecting effect as to the processing of the personal data already disclosed.

The EDPB finally underlines the requirement under Article 52(1) of the Charter of fundamental rights of the EU[15] according to which any limitations to the exercise of the rights and freedoms recognised by the Charter are subject to the principle of proportionality and may only be made if they are necessary. Therefore in order to be lawful under EU law, the draft provisions of the envisaged protocol

[13] The EDPB notes that the notion of emergency is referred to within the meaning of paragraph 1 of the draft provision on Emergency Mutual Assistance and considers that the scope of such situation may be further clarified and framed.
[14] See CJEU joint cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970 – par (120)
[15] See also Article 8(2) of the European Convention of Human Rights.

must fulfil this requirement. It then concerns both the personal data contained in the request as well as in the answer to such a request. **The EDPB is therefore particularly concerned by the wording of the draft Article 6(3) c) and of the draft explanatory report, paragraph 13 in relation to this provision, which seem to imply that requesting third countries Parties to the envisaged Protocol may not be bound to comply with the principle of proportionality when addressing requests to an EU Member State**. In addition, there is not full clarity on the possibility under these provisions to invoke the proportionality principle as a ground for refusal.

It is also unclear whether Parties would be bound by the obligations to ensure, in the context of the envisaged protocol, the conditions and safeguards set out in Article 15 of the Budapest Convention[16]. **The EDPB recommends clarifying that the obligations set forth under Article 15 of the Budapest Convention fully apply also in the context of this cross-border cooperation.**

**Provisions on data protection safeguards**

The EDPB considers essential that the provisional text made public is complemented by dedicated provisions on data protection safeguards, which must then be assessed together with other provisions, in order to ensure that 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.

The provisional draft provisions on request for domain name registration information and expedited disclosure of stored computer data in an emergency, 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. **In this regard the EDPB would again like to point out the necessity that the data protection safeguards apply to any exchange of personal data in the context of the envisaged Protocol[17], including in relation to the transfer of personal data[18].**

The EDPB considers that specific provisions on data protection safeguards must reflect key principles and in particular lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. Likewise, the EDPB would like to stress the importance of ensuring core individual rights (access, rectification, erasure), with any restrictions limited by the principle of proportionality, and of effective judicial redress for data subjects for violations of the data protection safeguards. Exercise of these rights also requires notification of the data subject, at least once this no longer puts at risk the investigation. These principles, rights and obligations are also in line with the modernised Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), to which many Parties to the Budapest Convention on Cybercrime are also Party. In line with Convention 108+, they should apply to all authorities processing the data in the requesting Party, in order to ensure the continuity

[16] See in particular Article 6(4) in brackets.
[17] Article 6(4) seems to limit the application of the safeguards as well as of Article 15 of the Convention to the information disclosed only and not to the personal data included in the request.
[18] According to the draft explanatory report, paragraph 9, the latter provision only may/should apply to the transfer of personal data pursuant to the joint investigations teams.

of protection. **The EDPB refers to its contribution in the public consultation in 2019 for further details on the EU requirements in this regard**[19].

**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.**

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[19] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf