30 April 2021

Access Now's comments on the draft 2nd Additional Protocol to the Budapest Convention on Cybercrime

Introduction

We thank the Cybercrime Convention Committee (T-CY) for the opportunity to provide comments to the draft 2nd Additional Protocol to the Budapest Convention on Cybercrime.[1]

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world.[2] We work on data protection and privacy around the world and we maintain a presence around the world, including in the policy centers of Washington DC and Brussels.[3] We are part of the Council of Europe consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) as an observer.[4] We are also a member of the EDRi network and support the contributions made by EDRi, including throughout the previous five consultations.[5]

In our submission, we will provide comments in several sections of the draft 2nd Additional Protocol, on the consultation process around this document, and on the relationship between this document and existing international and regional frameworks. Based on these comments, we invite the Cybercrime Convention Committee to continue the work on the draft 2nd Additional Protocol to the Budapest Convention on Cybercrime and revise the current text.

1. Consultation process

We call on the Cybercrime Convention Committee to reopen a period for comment and organise calls with civil society, data protection authorities, private sector representatives and states representatives to discuss modifications to the 2nd Additional Protocol before it is discussed at ministerial level.

Allowing for a three week period for public consultation on such an important document is far too limited. This is particularly problematic as most of the drafting meetings of the Protocol have been

[1] Cybercrime Convention Committee, Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime https://rm.coe.int/2nd-additional-protocol-budapest-convention-en/1680a2219c
[2] Access Now, https://www.accessnow.org/
[3] Access Now - About Us, https://www.accessnow.org/about-us/
[4] Council of Europe, List of observers of consultative committee on Convention 108 https://rm.coe.int/list-of-observers-nov-2018-en/1680938538
[5] EDRi, Council of Europe Second Additional Protocol to the Budapest Convention https://edri.org/our-work/cross-border-access-to-data-for-law-enforcement-document-pool/#budapest

held in closed sessions without the involvement of civil society and other experts whose contribution cannot be adequately represented. In addition, we note that many previous civil society comments shared through the EDRi network were not taken into account by the drafting group and that a large number of provisions that would negatively impact human rights remain part of the draft.
This deficient process does not reflect the principles of inclusiveness and transparency, the democratic values, and the protection of the rule of law promoted and upheld by the Council of Europe.

2. Impact on international agreements, constitutional protections and regional data protection norms

The draft 2nd Additional Protocol may risk impacting existing international agreements, constitutional protections and regional data protection norms.

As noted by the European Data Protection Board in its February 2021 statement on the Additional Protocol, since the Budapest Convention and its additional protocols are binding international instruments, 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".[6] This means that the final draft of the 2nd Additional Protocol should not be contrary to any Party constitutional and primary law and respect fundamental rights. Yet, in its current form, the 2nd Additional Protocol is not entirely compatible with the EU acquis in the area of data protection and the EU Charter for Fundamental Rights. In particular, the provisions of the 2nd Additional Protocol on data protection safeguards, data transfer, judicial remedy and oversights are highly problematic and would need to be re-assessed.

In addition, developments and implications linked to the draft 2nd Additional Protocol also risk bypassing Mutual Legal Assistance Treaties (MLATs). While we acknowledge deficiencies in the functioning of MLATs, these important frameworks should not be bypassed. We recall that work and solutions for the improvement of MLATs are possible and that these new solutions need to respect human rights principles.[7]

3. Data protection obligations

While a significant part of the scope of the Convention and of the 2nd Additional Protocol is related to data processing, we note that several Parties are not part of Convention 108 or 108+ of the Council of Europe on the protection of individuals with regard to automatic processing of personal data. This creates significant concerns in terms of the application and interpretation of safeguards across Parties to ensure that an adequate level of protection is guaranteed. All Parties involved in the discussion related to the 2nd Additional Protocol should be required to sign, ratify, and properly implement Convention 108+ of the Council of Europe.

---

[6] EDPB, Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) https://edpb.europa.eu/sites/default/files/files/file1/statement022021onbudapestconventionnewprovisions_en.pdf

[7] *See:* Access Now, blog series on the need to reform MLATs and proposed way forward https://www.accessnow.org/need-fix-broken-system-cross-border-data-access/

It is unclear how certain Parties will be able to comply with the requirements of Article 13 which reads as follows:

"In accordance with Article 15 of the Convention, each Party shall 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.****" (emphasis added)*

This Article shows that the 2nd Additional Protocol should be interpreted in line with national law providing for the protection of fundamental rights. Yet, a number of Parties, including the United States, do not have a comprehensive data protection framework. Other states may have provisions related to data usage in their domestic laws that are fundamentally in conflict with human rights and liberties. What is more, as we explain below in our submission, several provisions in this Protocol would run contrary to existing data protection laws and shall be modified or clarified.

Therefore, all Parties should develop comprehensive data protection measures and provide for the protection of human rights and liberties in their domestic system. We also recommend further improvements to the 2nd Additional Protocol to ensure the proper implementation and oversight of the data protection measures provided for under Articles 13 and 14.

For clarity, Article 14 of the 2nd Additional Protocol on protection of personal data should refer to key principles, in particular lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. We also support the recommendation made by the EDPB in its February statement which recall "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."[8]

Finally, Article 23 (3) of the 2nd Additional Protocol shall be amended as follows to ensure greater oversight over the application of the data protection measures (emphasis shows proposed amendment):

"The review of Article 14 shall commence once ten Parties to the Convention have expressed their consent to be bound by this Protocol. ***Independent oversight authorities, including data protection authorities and independent experts shall participate in this review."***

This review shall verify the implementation of data protection measures provided for in this Protocol and that the domestic law of assessed Parties provide for the adequate protection of human rights and liberties as established in Article 13. The outcome of these reviews shall be made public.

---

[8] EDPB, Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) https://edpb.europa.eu/sites/default/files/files/file1/statement022021onbudapestconventionnewprovisions_en.pdf

4. Judicial remedy and oversight

The requirements for judicial and non-judicial remedies presented under Article 14 (13) are limited. There is no indication of the necessary conditions that should be in place in each Party to clarify how access to these remedies mechanisms would be ensured. Case law from the Court of Justice of the EU on the right to effective remedy involving third countries have illustrated how different Parties may advance avenues for remedies that would not be considered as effective under the EU Charter of Fundamental Rights.[9] By not providing clear criteria for these remedies, the Protocol risks lowering the bar of these remedies and contradict EU law. Additionally, that language in Article 14 (13) shall clarify that remedies shall not only be effective but also available through transparent and independent systems.

Article 14 (14) refers to independent public oversight authorities that shall have "investigation powers and the ability to take corrective action" in order to ensure compliance with data protection measures. We recommend an addition to this paragraph to clarify that individuals have a right to lodge a complaint in front of these authorities in order to review compliance with processes as well as lawfulness of measures. The authority shall have the obligation to produce a decision on the basis of the complaint filed.

5. Data transfers

Article 14 (1) (d) says as follows:

"Each Party shall consider the processing of personal data pursuant to ***paragraphs 1.a and 1.b to meet the requirements of its personal data protection legal framework for international transfers of personal data, and no further authorization 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: (i) under the conditions set out in paragraph 15 when paragraph 1.a applies; or (ii) under the terms of an agreement or arrangement referred to in paragraphs 1.b or c, when one of those paragraphs applies."*

This provision affects the substantive and procedural conditions for transfer of personal data established under EU law. This provision effectively bypasses the conditions set forth under the international transfer chapters of the General Data Protection Regulation (GDPR) and the Police Directive (LED). While the EU legal framework seeks to guarantee a high degree of protection for personal data, this Protocol does not establish similar guarantees. Yet, it could create an area for the free flow of data between Parties based on limited safeguards and render the application of the LED and GDPR moot. This drastically contradicts the approach of the European Union to only allow transfer of personal data in cases where an adequate level of safeguards can be guaranteed and verified. The Protocol asks Parties to assume a level of protection that may well be nonexistent or weak in their domestic laws as we recall that a number of Parties involved in the discussion on the 2nd draft Additional Protocol do not have comprehensive data protection legislations. We therefore recommend deleting Article 14 (1) (d) and replacing it by a requirement that each Party

[9] CJEU, Case C-311/18, Schrems II https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6235979

assess, with the relevant oversight authority for data protection, the level protection of the requesting Party before allowing for transfers.

Finally, the draft 2nd Additional Protocol includes very little limitation with regard to the further processing and onward transfers of the transferred personal data by the requesting Party authority. We echo the recommendation made by the EDPB to "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."[10]

Conclusion

We invite the Cybercrime Convention Committee to continue the work on the draft 2nd Additional Protocol to the Budapest Convention on Cybercrime and revise the current text.

The current text does not provide for sufficient legal certainty and safeguards in the area identified in our submission. Most importantly, we believe a number of proposed measures would contradict important international human rights frameworks as well as regional legislation advancing people's rights, including the General Data Protection Regulation.

We look forward to continuing engaging with the Cybercrime Convention Committee through an increased and extended consultation process.

For more information
Please contact:

Estelle Massé
Global Data Protection Lead
(estelle@accessnow.org)

Raman Jit Singh Chima
Global Cybersecurity Lead
(raman@accessnow.org)

[10] EDPB, Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) https://edpb.europa.eu/sites/default/files/files/file1/statement022021onbudapestconventionnewprovisions_en.pdf