EuroISPA's comments on the draft text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime – 6th Round of consultations

EuroISPA is the voice of the European Internet industry, representing over 2.000 Internet Services Providers from across Europe, all along the Internet value chain. EuroISPA's members have long worked with judicial authorities in their countries of operation, and thus have valuable insights on the functioning of existing cooperation. Moreover, the overwhelming majority of EuroISPA's members are SMEs, and as such, face novel challenges from any new legal regime.

EuroISPA would like to share its comments on the full draft of the Second Additional Protocol to the Cybercrime Convention, that build upon the sets of comments shared during the previous rounds of consultations:

First of all, EuroISPA believes the draft is already on a good way to balance the interests of service providers and law enforcement authorities (LEAs). In particular, we support the consideration of the rights and obligations of enterprises, especially to safeguard the protection of customer data, and obligations and rights of authorities to prosecute, to protect in case of emergencies. Nevertheless, the draft still contains several points of concern.

General concerns in relation to Article 7

Our main concerns regard the introduction of direct cross-border production orders in Article 7. Considering the on-going discussions on the E-Evidence Regulation at an EU level[1] – and the variety of aspects that still remain unclear – we suggest refraining from prematurely adopting another provision on cross-border production orders in the Second Additional Protocol , before a thorough solution has been found in the EU. As the Second Additional Protocol would be open to signature to almost 40 additional states it is essential that both frameworks are harmonised. Otherwise, the parallel implementation of two separate legal regimes for inner-EU production orders on the one hand orders from third countries on the other will only lead to confusion and uncertainties on the side of the affected service providers and thus create significant challenges for the practical success of either legal framework.

Indispensable aspects to facilitate the cross-border data exchange between LEAs and ISPs

If direct cross-border production orders for subscriber information nevertheless remain in the text, then there are several key aspects to be considered to allow the technical implementation of cross-border orders. EuroISPA has already brought up these aspects in the past, but so far, they have not been recognized or have only been addressed vaguely. Therefore, we ask the T-CY to consider the experience

[1] Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (COM(2018) 225 final)

and expertise of ISPs in their cooperation with LEAs when finalizing the document in order to ensure the functioning of the legal regime in practice.

- The mandatory introduction of a unified electronic data exchange system

Unfortunately, at the moment Article 7 (6) only provides that "appropriate levels of security and authentication *may* be required" but leaves it to the Parties whether and which secure channels or means for transmission and authentication are available or whether special security protections are necessary. To ensure the secure and confidential exchange of information between law enforcement authorities and service providers is however essential to avoid data breaches and the leak of confidential information on on-going investigations and is thus indispensable for the success of the whole legal regime. Therefore, a high level of security should not be left to the sole discretion of the State Parties but be a prerequisite for making use of this provision. In any case, the use of unsecure transmission standards such as E-Mail should be avoided.

EuroISPA therefore encourages the T-CY to introduce a unified electronic data exchange system, which is compatible to the most used systems in the EU or provides technical interfaces to them (e.g. for telecom providers via ETSI-standards), in order to support the secure and efficient transmission of data requested. Such a system will not only ensure security and integrity in the data transmission process but also significantly determine the ability for ISPs to verify the authenticity of a production order under Article 7. This will allow service providers to respond more rapidly to foreign requests compared to the situation currently foreseen, where a service provider would have to determine the authenticity based on the E-Mail address used for sending the request or production order which cannot always be verified and easily be imitated for fraudulent means.

Where the affected service providers already have a secure system for data transmission in place such a system should be used instead as long as their systems enable the identification and authentication of sender and receivers and ensure data integrity.

- The drafting and subsequent use of templates

EuroISPA has already stressed in its response to the previous rounds of consultations that it is imperative to foster the use of templates for cross-border orders and requests, to accelerate the requesting process and minimize the risk of mistakes and legal uncertainty. Aspects like pointing out the voluntary nature of a response to a request under Article 6 and precise specifications on language requirements, are necessary.

- The installation of a single point of contact (SPOC)

Article 8 (11) already provides the option for State Parties to require that requests are to be submitted by the central authority of the requesting party. Already in its past contributions, EuroISPA has pointed out the benefits of a single points of contact (SPOC) for issuing production orders to service providers. In particular, ISPs currently receive a large number of informal requests on technical issues prior to receiving a production order. This could be avoided if all requests are transmitted via a SPOC which has the necessary technical and legal know-how in respect of how to request data from service providers. Therefor a similar provision on making use of a central authority should also be included in Articles 6 and 7. This SPOC would also serve as the central point for the electronic data exchange system.

- Ex-ante review of a production order under Article 7 by a judge or other independent authority

Without any requirement of an ex-ante review of a cross-border request by a judge or other independent authority, the entity receiving the request would not be sure whether it is in accordance with domestic

laws, requiring them to assess the legality of the requests autonomously in order to avoid that they are held liable for disclosing information unlawfully.

Additionally, under most legal frameworks, even the disclosure of subscriber information requires, at least, the order of a public prosecutor. However, under the wording of Article 7, any "competent authority" could issue a cross-border production order, which would entail that the threshold under which a service provider must disclose user data would be lower for foreign orders than for domestic ones. In addition, both the case law of the CJEU and the ECtHR clearly stipulate that production orders concerning stored user data must undergo a prior review by an independent authority, something that has recently been confirmed again by the CJEU in its judgement *Prokuratuur.*[2] .

EuroISPA therefor requires, that the ex-ante review by a judge or an independent authority should not be left to the discretion of the State Parties, as is currently foreseen in Article 7 (2)b, but rather be mandatory.

- Exclusion of SMEs

Considering the low number of requests to small and medium-sized (SMEs) service providers, the personnel and financial costs which come along with the implementation of Articles 6 and 7 appear to be unproportionate.

For this reason, EuroISPA calls for an exclusion of SME enterprises from the scope of the Second Additional Protocol. This would, at the same time, not impede criminal proceedings as for the information held by these SMEs could still be requested by using one of the other channels which the Second Additional Protocol provides. As the number of requests to SMEs will be significantly low, such a solution would also not overload the capacity of these channels.

- Cost reimbursement in the receiving Party

Unfortunately, the draft only includes a provision on cost reimbursement for video conferencing but does not include any reference to the immense financial and personnel investments incurred by the service provider. Rather, it seems that it will stay at the discretion of the parties to provide cost reimbursement if provided so under their national law. This will not only lead to an imbalanced system, where states without national provisions on cost reimbursement can benefit from the assistance of foreign service providers without having to come up for their expenditures but also to uncertainties in practice. Even if there is a cost reimbursement provision in the legal framework of the requesting state, in practice, the concrete procedure under which a foreign service provider could request such reimbursement would still be unclear. Besides, experience in states which have a cost reimbursement system in place has shown that it works as an efficient barrier against unjustified bulk requests for data, limiting the number of requests to what is strictly necessary, which will equally contribute to the success of the system.

EuroISPA therefore requests, that cost reimbursement is provided by the State Party in which the service provider has its seat. This state could then reimburse itself at the requesting state.

[2] Case C-746/18 *H.K v Prokuratuur* [2021] ECLI:EU:C:2021:152; see also: ECtHR Szabo v Hungary App no 37138/14 (ECtHR 12 January 2016), Benedik v SloveniaApp no 62357/14 (ECtHR 24 April 2018)

Definition of "provider's possession or control" in Articles 6 to 9

It remains unclear whether information in a services provider's "possession or control" under Articles 6, 7, 8 and 9 includes also data held by a subsidiary of the service provider on foreign territory, such as is the case under the doctrine of "possession, custody and control" under US law.

Under such an interpretation, several significant challenges would arise, most importantly however, the domestic authorities of the state where the subsidiary has its seat would appear not to be involved in the process and therefore, the respective safeguards, particularly those in Art 7 (5), would not be applied.

For this reason, EuroISPA demands that production orders are always addressed to the service provider holding the contractual relationship with the customer whose data is concerned.

Principle of proportionality requires an exemption for MSMEs regarding the 24/7 network

EuroISPA believes that the principle of proportionality requires an exemption for micro, small and medium sized enterprises regarding the 24/7 network, to prevent that providers can be forced by national law to answer requests in emergency cases also in 24/7 manner. Otherwise, these categories of enterprises will be overstrained. Thus, in the explanatory report regarding Article 9 or in the Article itself such an exemption is to be foreseen.

Protection of personal data (Article 14)

As a preliminary remark, EuroISPA regrets the lack of any explanatory report to this provision as it impedes a thorough analysis.

- <u>International data transfers (Sub-paragraph 1 (d)):</u>

The wording proposed is unclear as on the one hand, it stipulates that the disclosure of personal data based on the Second Additional Protocol shall be considered "to meet the requirements of data protection frameworks for international data transfers" and shall need "no further authorization". On the other hand, the following sentence foresees that a party may (only) refuse data transfers under the terms of an agreement – including data protection agreements. Consequently, it remains unclear to what extent the disclosure of personal data which falls under the scope of the GDPR to a law enforcement authority in a third country, would be permitted.

In general, whether or not a data transfer by a service provider in response to a foreign production order is in line with the GDPR's requirements for data transfers to a third country cannot be clarified in a specific provision of the Protocol but must rather be assessed based on the question, whether the treaty as such can serve as a legal basis and whether it provides the minimum safeguards that ensure the requirements stemming from EU data protection law are complied with.[3]

Considering that the Protocol is not directly applicable for neither the concerned service providers nor the affected users, this assessment will also have to consider the national implementation of the safeguards foreseen in Article 14. Nevertheless, it should be avoided that it is left to the service providers concerned to carry out this legal assessment on a case-by-case basis, as is currently foreseen in the aftermath of the *Schrems II* decision[4], as this burden would exceed the capacities of a service provider, in particular such without any legal department of their own.

[3] CJEU opinion 1/15 [2016] ECLI:EU:C:2017:592 para 141

[4] Case C-311/18 *Data Protection Commissioner v Maximilian Schrems and Facebook* [2020] ECLI:EU:C:2020:559