EuroISPA's comments on the provisional text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime

EuroISPA is the voice of the European Internet industry, representing over 2.500 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.

As the 4th round of consultations on the 2nd Additional Protocol to the Cybercrime Convention approaches, which aims to set out new rules to improve the cooperation in respect to cross-border access to electronic evidence, EuroISPA would like to share its comments on the draft provisions.

1. Strong preference for the procedure provided in section 5

Although EuroISPA acknowledges the possible benefit of a seek procedure under section 4, it believes that to offer the highest level of legal certainty, the procedure provided in section 5 should be the norm for the disclosure of subscriber information since the authorities in the country of the receiving party are much stronger involved. This would bring more legal certainty on the side of the service providers and, notwithstanding the ability of providers to voluntarily perform additional checks of received inquiries from LEAs, will contribute to better safeguarding the rights of their users. Especially considering that more than twice as many states have signed the Budapest Convention as there are EU Member States, an additional legal basis for cross-border orders should be avoided. Also, it should be first assessed how the parallel discussed E-Evidence Regulation on an EU-Level will be implemented. A preference of the procedure under section 5 would not affect the voluntary disclosure of information by service providers to law enforcement agencies in third countries.

Recommendation: EuroISPA suggests to strongly question section 4 and apply section 5 procedures to the disclosure of subscriber information. If section 4 should nevertheless be maintained, then the following recommendations should be taken into account.

2. Double criminality requirement

EuroISPA welcomes the introduction of procedural and material safeguards in the draft. We believe however that it would benefit from furthermore adding the requirement of double criminality. According to both section 4.5.c (5) c and section 5.8., the receiving state can refuse to comply with an order by another party based on the grounds established in Art 25 (4) and Art 27 (4) of the Budapest Convention, which lay down the reasons to refuse a response to a Mutual Legal Assistance ("MLA") request. According to our information, these have been used to invoke double criminality concerns hitherto by receiving authorities.

Nevertheless, and in order to provide legal clarity on this important issue there should be a clarification – at least in the explanatory report to the protocol – that double criminality is a legal requirement for all production orders under section 4 and 5. Therefore a receiving service provider should equally be able to refuse the disclosure of user data based on Art 25 (4) and Art 27 (4) Budapest Convention.

Recommendation: EuroISPA requests to be clarified that double criminality is required for all production orders under section 4 and 5 and that service providers are permitted to refuse orders which do not fulfil based on Art 25 (4) and Art 27 (4) of the Budapest Convention.

3. Definition of data categories

EuroISPA generally agrees to the clear distinction between subscriber data and traffic data. However, we have reservations regarding the definition of subscriber information in the explanatory report, which uses a very broad interpretation of the term subscriber information in Art 18 (3) Budapest Convention (CCC), and in particular includes IP-addresses and subscriber information to an IP-address. Such an interpretation clearly does not follow from the wording in Art 18 (3) CCC and is also not in accordance with several parties' legal systems, in which the conditions to obtain IP-addresses differ from those to obtain basic subscriber information such as name, address and contact details as has been found as well by the T-CY.[1]

EuroISPA considers the disclosure of IP-addresses to constitute a more intrusive measure than that of basic subscriber information. This has also been confirmed by the ECtHR in the case of *Benedik v Slovenia*[2] in which the Court found that when assessing the intrusiveness of the disclosure of an IP-address one must keep in mind, that it reveals a good deal about the online activity of an individual, including sensitive details of his or her interests, beliefs and intimate lifestyle. This argument is particularly true as regards temporary IP-addresses which a service provider assigns to a user's device every time he or she connects to the network (dynamic IP-address). In order to disclose the name to such an IP-address, the service provider must process additional metadata to determine who used the specific IP-address at a given time. For that reason, the ECtHR has also clearly distinguished between dynamic IP-addresses and subscriber information in *Benedik v Slovenia*. The same is true for log-on IP addresses to certain platforms,[3] since already the information, that different user accounts have logged on to a platform using the same IP-address can provide significant information about their relationship and location.

[1] Cybercrime Convention Committee T-CY discussion paper: Conditions for obtaining subscriber information–static versus dynamic IP addresses T-CY (2018)26 p. 6

[2] *Benedik v Slovenia* App no 62357/14 (ECtHR 24 April 2018)

[3] The IP-address used when logging on to a specific platform

It follows that subsuming the disclosure of IP-addresses under section 4 would violate the jurisprudence of the ECtHR and therefore also not be in accordance with the argument in the explanatory report to section 4 according to which subscriber information does not allow precise conclusions concerning the private lives of individuals.

Recommendation: As the definition of subscriber information stems from the original text of the Cybercrime Convention (Art 18 (3)), we recognize that it is unlikely to be changed in the text of the 2nd Additional Protocol. We therefore believe that the scope of section 4, which concerns the direct cross-border disclosure of subscriber information, should instead clearly exclude the disclosure of at least dynamic and log-on IP-addresses which would make the scope in line with the argued low intrusiveness in the explanatory report.

If IP-addresses are nevertheless kept in the scope of section 4, EuroISPA recommends deleting at least the "quid-pro-quo" provision in 4.1.9., according to which a party - that excludes access numbers from the scope of cross-border production orders on subscriber information - is not permitted to issue orders for such numbers under paragraph 1 to service providers in other parties' territories. Parties, whose legal system requires a different treatment of IP-addresses compared to basic subscriber information would otherwise see themselves facing a difficult and unpopular decision, which potentially would limit the application of this exception severely in practice, thereby endangering the protection of fundamental principles of several legal systems.

4. Notification procedures to the receiving State should be enhanced

EuroISPA takes note of the intention that receiving parties are provided with the option of either to require notification by the requesting authority to the authorities in the receiving state or consultation by the provider with their competent authorities when a provider receives a cross-border order under section 4. However, it is unclear why such an important additional safeguard that provides legal certainty for both the service provider and the affected user shall be left to the discretion of each party to be implemented. Besides, the consultation procedure, which provides a more active role of both providers and authorities in the receiving state can only be invoked under 'certain circumstances' that have to be pre-defined. In particular, this requirement of defining abstract rules under which the consultation procedure can be invoked risks that in practice it would not be used in all cases where necessary. Additionally, the consultation obligation could be inflicted upon the providers.

Recommendation: EuroISPA demands that the competent authorities in the receiving party shall be notified in all circumstances as this would provide more legal certainty whereas preference is given to notification already by the requesting party to the receiving party, in order to avoid additional burden for the service provider. Authorities in the receiving state should be involved as to ensure that rule of law in the receiving state is applied.

5. User Notification as default setting

EuroISPA recognizes, that in the current draft, user notification is generally considered permissible where not prohibited under the domestic law in the receiving state. As indicated in para 17 of the explanatory report to section 4, the responsibility to be aware of the applicable law of the receiving state and the service provider's policies concerning user notification therefore lays with the requesting authority. Considering however, the importance of user notification for enhancing transparency of production orders and allowing the affected individual to exercise his or her procedural rights, user notification should not only be permissible but rather required as the default setting.

Recommendation: EuroISPA advocates for user notification to be the default setting. Moreover, in case a 'gag-order' is attached to the production order, it should be possible for the service provider to ask for additional information. However, in no case should the service provider become liable for not performing such verification.

6. Cost reimbursement for expenses incurred

EuroISPA regrets that the draft text does not include any reference to how the investment and costs of data disclosures incurred by service providers will be dealt with.

Recommendation: EuroISPA believes that cost reimbursement for investment and the reimbursement for costs associated with data disclosure should be clearly defined in the draft text. The reimbursement provisions should be designed in a way that does not suppose a burden for ISPs and should not be left to the sole discretion of the parties. Such a provision would also serve as an incentive for authorities to limit the number of requests to what is strictly necessary.

7. Harmonised timeframes for responding to orders under sections 4 and 5

EuroISPA welcomes the adequate timeframe of 30 days for responding to a cross-border production order under section 4. It is however unclear, why the timeframe for the disclosure of the same data category is limited to 20 days when responding to a foreign order that has been given effect under national law according to section 5.

Recommendation: In order to provide a streamlined system for providers, EuroISPA recommends harmonising the timeframes and define a general timeframe of 30 days for the disclosure of all subscriber data.

8. Exceptions for SMEs should be included

Whereas the obligations included in the draft were drafted primarily with large service providers in mind, the provisions have to equally be implemented by all small and medium-sized providers (SMEs). SMEs substantially contribute to the functioning of the internet eco-system but often do not have the necessary financial and personnel resources to comply with these obligations in the same way as a large service provider. For this reason, and in order to avoid that small and medium sized providers are unproportionally affected by these new provisions, exceptions and limitations for SMEs should be included.

Recommendation: EuroISPA demands the provision of separate and more practical timeframes for SMEs to respond to disclosure requests.

9. Secure data transmission

The appropriate levels of security and authentication needed to accept the request are not defined in the protocol. While parties may require a certain secure transmission route, no general thresholds or standards are provided. In order to enhance both law enforcement authorities' and service providers' ability to securely and efficiently transmit data, a voluntary data exchange system should thus be established, which would furthermore facilitate the authentication process as well.

Where service providers already have a secure system for data transmission in place, they should however be allowed to maintain these portals for Parties to submit access requests if their systems enable the identification and authentication of sender and receivers and ensure data integrity.

Recommendation: EuroISPA recommends the development of a platform as a voluntary good practice example, which allows the secure and confidential exchange of data between ISPs and the requesting party.

10. Prior review by an independent authority

The current draft leaves to the discretion of the parties to require that every cross-border order must be issued by, or under the supervision of a prosecutor, judicial authority or otherwise be issued under independent supervision.

Providing sufficient discretion to the parties to allow them to keep up their traditional way of requesting data in criminal proceedings is prima facie comprehensible. Nevertheless, both the case law of the CJEU[4] and the ECtHR[5] clearly stipulate the requirement of a prior review of production orders in respect of stored user data by an independent authority. Considering that e.g. under US law, subscriber information can be obtained by a simple administrative subpoena without any prior judicial oversight[6] this requirement would not be fulfilled by all parties to the convention. Instead of allowing a levelling down of procedural

[4] Joined Cases C-203/15 and C-698/15 *Tele 2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson* [2016] ECLI:EU:C:2016:970

[5] *Szabo v Hungary* App no 37138/14 (ECtHR 12 January 2016)

[6] 18 U.S.C. § 2703(c)

safeguards in the agreement we request the Council of Europe to uphold the legal standard developed by Europe's two highest courts.

Recommendation: EuroISPA recommends amending section 4.1.2. and making the review by an independent authority an obligation. Besides, it must be clarified, that such a review has to be conducted prior to sending the production order to the service provider.

11. Better definition of "possession and control" of data

The draft text refers in section 4 to data which is in a service provider's 'possession and control'. The Explanatory Report of the Budapest Convention interprets 'possession' of the data by referring to data stored in the ordering party's territory whereas for 'control', the report only requires that the person can produce the data from inside the ordering party's territory, as for instance when using remote data storage facilities. According to the T-CY's Guidance Note on Art 18 CCC, the actual storage location of subscriber information is therefore irrelevant as long as the data is in the 'possession or control' of the provider receiving the production order.

Different to the location of the data, it is unclear whether "possession and control" includes however also information held by a subsidiary on foreign territory. With regards to production orders under Art 18, the explanatory report stipulates that data must be produced from within the ordering party's territory. It is unclear, how this corresponds with this new norm, i.e. whether the data must in this case be produced within the ordered ISPs territory.

In this context also the broad definition of 'possession, custody and control' under US law should be taken into account, where it clearly includes also such data, which is held by a subsidiary on foreign territory. Considering that under legal frameworks such as the GDPR, service providers underly strict rules in relation to transferring personal data to third countries, any such interpretation should be avoided in the protocol, as this would otherwise lead to severe legal conflicts for the affected companies, in particular where the state in which the subsidiary is based is not part of the treaty or has not opted for this provision.

Recommendation: EuroISPA suggests the inclusion of a more precise definition of what data is in the provider's "possession and control" in order to prevent any conflicts with other laws, in particular data protection requirements and to not leave companies in legal uncertainty. Besides, consistency of the terminology used with other relevant international processes on cross-border access to electronic evidence must be ensured contradiction between them be avoided.

12. Voluntary proportionality check

According to para 15 of the Explanatory Report to section 4, no summary of facts shall be provided. Under some jurisdictions, providers however can be held responsible for disclosing information outside legal requirements.

Recommendation: EuroISPA suggests that a rough summary of the facts to a cross-border order under section 4 can be requested by the provider on a voluntary basis, in order to be able to conduct additional proportionality checks when deemed necessary.

This will not entail in any case that service providers are the responsible actors to ensure conformity with the requesting state's laws, nor should they be held liable for not having carried out additional checks. In case providers find that the proportionality is not given, they should be allowed to refuse the order.

13. Mandatory transmission via a SPOC

According to the current draft, cross-border orders under section 4 could in principle be issued by any law enforcement authority of a party which has the competency under domestic law. However, EuroISPA's experience shows that having one single point of contact (SPOC) facilitates and accelerates the process and adds security to both parties. 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.

Recommendation: All orders under section 4 should be transmitted via a SPOC. Besides, a similar provision should also be provided for orders under section 5, where 5.10. currently only leaves that to the discretion of the receiving party.

14. Provision of templates

In order to accelerate the requesting process and to minimize the risk of mistakes and legal uncertainty, the use of templates for cross-border orders under section 4, such as are provided in the Annex to the EU Commission's proposal for a regulation on cross-border access to e-Evidence should be promoted. In order to avoid the parallel use of different templates, the Council of Europe should coordinate in this aspect with the EU Commission.

Recommendation: Add templates for cross-border orders under section 4 as an Annex to the Second Additional Protocol.

15. Language requirements should be further specified

The current text of section 1 on languages does not match with section 4 on cross-border orders which are directly addressed to ISPs. Precise language requirements are however desirable, in particular, in which languages ISPs should receive such orders, in which languages they can raise questions for clarifications to the ordering authority etc

Recommendation: EuroISPA requests further clarification and specification of the language requirements with regards to cross-border orders.

16. "Emergency" must be defined narrowly to avoid undermining the efficiency of the provision

Section 3.1 defines an emergency as any situation in which there is a significant and imminent risk to the life or safety of a natural person. However, a risk to the safety of a person can however be interpreted rather extensively, covering also several non-life-threatening situations. If every request is described as an emergency, none is treated like such and MLA procedures are not accelerated.

Recommendation: EuroISPA requests a narrower definition of an emergency situation in order to allow the emergency MLA to properly unfold its potential in respect of cross-border cooperation in criminal matters.