Council of Europe Cybercrime Convention Committee (T-CY)
Avenue de l'Europe 1
67000 Strasbourg
France

ISPA AUSTRIA'S CONTRIBUTION TO THE PUBLIC CONSULTATION ON THE PROVISIONAL TEXT OF THE SECOND ADDITIONAL PROTOCOL TO THE BUDAPEST CONVENTION ON CYBERCRIME

ISPA – Internet Service Providers Austria welcomes the opportunity to provide comments to the draft provisions of the Second Additional Protocol to the Budapest Convention on Cybercrime. We are a voluntary business representation and act as the voice of over 220 internet service providers from various fields all along the internet value chain. ISPA Austria's members have long worked with judicial and law enforcement authorities and thus have valuable insights in the functioning of existing cooperation. Moreover, the majority of ISPA members are SMEs, and as such, face novel challenges from any new legal regime. We have followed the work of the Council of Europe with great interest over the years and value its expertise in the field of Cybercrime and other internet related topics. In our role as the voice of the Austrian internet industry we would like to address the following aspects of the draft text and provide recommendations where appropriate.

Section 1 – Languages

The current text of section 1 on 'languages of requests' only refers to language requirements of requests sent to other parties' authorities and does not cover direct requests to service providers such as provided in section 4 of the draft.

Direct cross-border orders raise however several additional language-related questions. In particular, it is essential to clearly define in the protocol the languages in which a service provider may be addressed in a cross-border order and whether the service provider would similar to state parties be allowed to define certain languages as acceptable in addition to the official language of the state where it is registered. In this context it should also be clarified that a service provider is not obliged to accept requests in each language which the state it is established in has determined acceptable. On top of that it is important to provide guidance on the language requirements for further inquiries by the service provider which may be necessary due to unclear orders or failed translations.

ISPA Austria thus requests the Committee to further clarify these issues in the protocol which would contribute to a much smoother application in practice. In particular ISPA Austria encourages the inclusion and use of templates and forms, as further explicated below, which may serve as well to solve several of the aforementioned language-related questions.

Section 3 – Emergency mutual legal assistance

1) **An 'emergency' must be defined narrowly to avoid undermining the efficiency of the provision**

According to section 3.1. an 'emergency' means any situation in which there is a significant and imminent risk to the life or safety of a natural person. A risk to the safety of a person however can be interpreted extensively, since also several non-life-threatening situations are imaginable which still constitute a risk to the safety of a person.

In practice this may cause law enforcement agencies, in order to receive swift responses, to routinely add to each MLA request that an assumed imminent risk to the safety of a person exists. Even in those cases in which am emergency does not exist, the receiving authority must nevertheless assess the request accordingly which eventually may even lead to additional work on the side of the receiving state and thus would only marginally speed up the proceedings.

ISPA Austria thus recommends a narrower definition of an 'emergency', since if every request is described as an emergency, none is treated like such.

2) **Further ways to speed up MLA procedures should be considered**

Except for the suggested emergency MLA procedure there are several other ways for speeding up the current process. Examples include a full digitisation of the MLA process and the avoidance of using old transmission technologies such as Fax, which in several states is still the primarily used technique but delays the procedure significantly. Fax requests often must be typed into a computer system by hand and may lead to misapprehensions on the side of the receiver due to unreadable print outs.

Besides, increasing the personnel and financial resources of the competent authorities in the receiving states and the installation of single point of contacts (SPOCs) in both states with the necessary technical and legal know-how will further accelerate the process.

Whereas the provision of additional resources is at the full discretion of the parties, the digitisation of the process could also be encouraged by respective provisions in the protocol which would require states to use a fully digitised system when processing MLA requests. In addition to that, ISPA Austria encourages the Council of Europe to use its broad expertise in the field of criminal investigations in the digital sphere to issue guidelines for LEAs and contribute to a better education of the competent staff for handling MLAT requests on the LEA side.

Section 4 - Direct disclosure of subscriber information

1) We encourage the Committee to refrain from creating a new legal basis for cross-border production orders

As a preliminary remark, ISPA Austria believes that to offer the highest level of legal certainty, the Council of Europe should refrain entirely from introducing a new regime for direct cross-border orders under section 4 and rather rely on the suggested procedure in section 5 in which the authorities in the receiving party are much stronger involved. This would bring more legal certainty on the side of the service providers and also contribute to better safeguarding the rights of their users.

Considering in particular that more than twice as many states have signed the Budapest Convention as are EU Member States, an additional legal basis for cross-border orders should be avoided and first be assessed, how the parallel discussed Regulation on European Production and Preservation Orders for electronic evidence in criminal matters will be implemented on an EU-level.

If section 4 should be maintained nevertheless, then the following recommendations should be considered:

2) The disclosure of IP-addresses is more intrusive than basic subscriber information and should be excluded from the scope of section 4

The scope of cross-border orders under section 4 is limited to subscriber information, which is defined in Art 18 (3) of the Budapest Convention (CCC) and includes also 'access numbers'. The explanatory report to section 4 which refers to this definition provides a very wide interpretation of access numbers, covering also IP-addresses, in particular log-on IP-addresses to a specific account, the IP-address used to create an account, or the IP-address used at a specific time.

Such an interpretation does not follow directly from the wording in Art 18 (3) CCC. In particular it should be taken into account that in the explanatory report to the Convention, IP-addresses are mentioned as a clear example for traffic data, not subscriber information, as they indicate the origin of a communication process.[1]

Subscriber information on the other hand means information that is directly related to the subscriber. Considering the examples which are listed in Art 18 (3) CCC, which only include information that is permanently assigned to a specific individual, it follows that also only such access numbers that are permanently assigned to a certain subscriber, as is the case with a static IP-address can be considered subscriber information.

The disclosure of non-static IP-addresses, in particular any form of disclosure of temporary IP-addresses which a service provider assigns to a user's device every time he or she logs on to the

[1] Council of Europe, 'Explanatory Report to the Convention on Cybercrime' (2001) CETS No. 185 para 30

network (dynamic IP-address) must fall under the regime of the disclosure of traffic data. In order to disclose the name to such an IP-address, the service provider must process additional sensitive metadata to determine who used the specific IP-address at a given time whereas already processing this sensitive data constitutes a significant interference with the user's right to privacy. Subsuming non-static IP-addresses thus under the term 'subscriber information' does not seem to support 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. Likewise, an interference may occur when disclosing the log-on IP-addresses to certain platforms, as already disclosing 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.

Allowing the disclosure of IP-addresses under the same conditions as subscriber information is moreover not in accordance with several parties' legal systems, in which the respective conditions differ substantially as has been found as well by the T-CY in a recent report.[2] On top of that, the fact, that the disclosure of IP-addresses constitutes a more intrusive measure than that of basic subscriber information has also been confirmed by the European Court of Human Rights in the case of *Benedik v Slovenia* 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.[3]

As the definition of subscriber information stems from the original text of the Cybercrime Convention it is unlikely to be changed or specified in the text of the Second Additional Protocol. Instead, non-static IP-addresses should explicitly be excluded from the scope of section 4 and direct cross-border production orders be limited to the disclosure of basic subscriber information.

If IP-addresses are nevertheless kept in the scope of section 4, ISPA Austria suggests deleting at least the 'quid-pro-quo' provision in section 4.1.9, according to which a party which excludes access numbers such as IP-addresses from the scope of cross-border production orders on subscriber information is not permitted to issue orders for such information under paragraph 1 to service providers in other parties' territories. Parties, whose legal system requires a different treatment of IP-addresses would otherwise be under pressure not to uphold their privacy standards in this respect which would limit the application of this exception severely in practice and consequently threaten fundamental principles of several legal systems.

3) Every production order must be issued by or under the prior supervision of an independent authority

According to section 4.1.2b the draft currently leaves it 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.

[2] Cybercrime Convention Committee T-CY discussion paper: Conditions for obtaining subscriber information–static versus dynamic IP addresses T-CY (2018)26 p. 6
[3] *Benedik v Slovenia* App no 62357/14 (ECtHR 24 April 2018) para 109

Providing sufficient discretion to the parties allowing them to keep up their traditional way of requesting data in criminal proceedings is prima facie coherent. Nevertheless, both the case law of the CJEU and the ECtHR clearly stipulate that production orders concerning stored user data must undergo a prior review of by an independent authority.[4] Considering that e.g. under US law, subscriber information can be obtained by a simple administrative subpoena without any prior judicial oversight this requirement would not be fulfilled by all parties to the convention. Instead of allowing a levelling down of procedural safeguards for accessing personal data in the additional protocol we request the Council of Europe to uphold the legal standard developed by Europe's two highest courts and turn the current opt-in provision into an obligation.

Section 4.1.2. should therefore be amended accordingly and further clarify that such a review must be conducted prior to sending the production order to the service provider.

4) The principle of double criminality must be upheld

ISPA Austria shares the opinion that including an additional provision on the principle of double criminality would be beneficial, which requires that the conduct under investigation is a crime in both the requesting and the receiving party. In the current draft, according to 4.1.5.c (ii) the receiving state can order the service provider to refrain from the disclosure of information 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 and have been used to invoke double criminality concerns hitherto.

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.

5) A secure data transmission system should be required

Secure and confidential transmission of information between law enforcement authorities and service providers should be one of the preliminary goals as otherwise there is an immanent risk of data breaches on the side of the service provider and the leak of confidential information on on-going investigations on the side of the law enforcement authorities. These concerns are reinforced by the fact that if implemented in the current form, thousands of ISPs and law enforcement authorities from potentially over 50 countries with different security and data protection standards would have to cooperate with one another.

[4] See CJEU 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 and ECtHR *Szabo v Hungary* App no 37138/14 (ECtHR 12 January 2016), *Benedik v Slovenia* App no 62357/14 (ECtHR 24 April 2018)

However, surprisingly in its current form the draft text of the protocol only stipulates that parties *may* require 'appropriate levels of security and authentication' for receiving an order from another state but does not provide any concrete thresholds. Other than in respect to the transmission of data between two state parties, also no reference is given to the use of encryption technology as a way to safeguard security. Besides, according to the explanatory report, already the use of an 'official e-mail address' shall be considered as a sufficient method of authentication. ISPA Austria strongly opposes this view, since on the one hand, a service provider will not always be able to verify each E-Mail domain and on the other hand, E-Mail addresses can easily be imitated for fraudulent means.

In order to ensure the secure, confidential and efficient transmission of information, the protocol should not leave the aspect of a secure transmission to the sole discretion of parties, but rather stipulate a voluntary secure and encrypted data exchange system, which would also facilitate the identification and authentication processes and ensure the integrity of data. Service providers which already have such a system in place should be allowed to maintain these portals for parties to submit access requests if their systems enable the above-mentioned requirements sufficiently.

6) Clear data protection safeguards must be included

When transmitting information to a law enforcement agency in a non-EU country, a service provider which falls under the scope of the GDPR conducts a data transfer to a third country. For such to be in accordance with the GDPR it must have a clear legal basis and comply with the provisions in Chapter V GDPR. As regards the latter, it follows from Article 48 GDPR, that data transfers to third countries can be based on an international agreement such as the envisaged Second Additional Protocol to the Budapest Convention. However, it is still essential that the agreement ensures that the level of protection under the GDPR does not get undermined, as previously found by the CJEU in its opinion on the PNR-agreement between the EU and Canada.[5]

Although the Budapest Convention already contains a general provision that the application of all powers granted therein are subject to conditions and safeguards that shall provide for the adequate protection of human rights, it must be recalled that according to the CJEU, an agreement which entails the transfer of personal data to a third country must itself provide minimum safeguards that ensure that the requirements stemming from EU data protection law are complied with.[6] Hence, considering that the Cybercrime Convention lacks any such data protection safeguards for data transfers, it cannot be considered to fulfil this criterion and data transfers in accordance with the Second Additional Protocol would be unlawful, even where stipulated by national law. ISPA Austria is aware that the Committee plans to add additional provisions on safeguards to the protocol. Until these are made public, no full assessment of the agreement is however possible.

[5] CJEU opinion 1/15 [2016] ECLI:EU:C:2017:592
[6] Id. para 141

Considering that in practice it would be the service providers who have to deal with the complaints of its users, ISPA Austria calls upon the Council of Europe to include clear data protection safeguards in the agreement, which fulfil the high standard required by the CJEU in its previous jurisprudence. This is furthermore essential in order to avoid that data transfers under the agreement would be declared unlawful under the GDPR regime in the future, which would create similar turmoil among companies as after the annulment of the Safe Harbour agreement in 2016.[7]

7) A provision on cost reimbursement is necessary

The draft text 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 unbalanced 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 practical uncertainties. For instance, even if there is a cost reimbursement provision in the legal framework of the requesting state, it would remain unclear how a foreign provider could receive cost reimbursement, which language it must use etc.

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 and will thus limit the number of requests to what is strictly necessary.

ISPA therefor suggests that an explicit provision on cost reimbursement should therefore be added to section 4 as has also been included in section 2.5. on video conferencing.

8) The timeframe for responses should be streamlined to 30 days

ISPA Austria generally 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.

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

[7] Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2016] ECLI:EU:C:2015:650

9) A precise definition of what data is in the provider's 'possession and control' is necessary

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 as referring to data stored in the ordering party's territory whereas for 'control', the report only requires that it can be produced from inside the ordering party's territory, as for instance when using remote data storage facilities. According to the 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 however unclear whether 'possession and control' includes also information held by a subsidiary on foreign territory. In this context the broad definition of 'possession, custody and control' under US law should be taken into account, where it includes also data that is held by a subsidiary on foreign territory. Considering that under 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.[8]

ISPA Austria therefor 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 and contradiction between them be avoided.

10) Service providers should be allowed to request a rough summary of the facts for proportionality checks

According to para 15 of the explanatory report to section 4, no summary of facts shall be provided to the service provider due to confidentiality concerns. Since in some parties, service providers may be held liable for compliance with an unlawful order, it should be possible for the provider to request a rough summary of the facts. This would enable service providers, when deemed necessary, to perform additional proportionality checks on a voluntary basis.

In any case this should not entail that service providers are in general the responsible actors to ensure conformity of an order with the requesting state's laws. In particular, a service provider should not be required to act as a guarantor for safeguarding fundamental rights which lays outside the abilities of corporations, in particular SMEs.

[8] According to Article 48 GDPR, any transfer of personal data by a provider subject to the GDPR to a controller or processor not subject to the GDPR in a third country which is based on a foreign judgment or administrative decision – such as a production order - is only allowed where based on an international agreement.

In order to provide the necessary flexibility in this regard we thus recommend amending para 15 of the explanatory report to section 4 and add that although no summary of facts is required when transmitting the order to the service provider, a service provider can nevertheless request a rough summary after receiving the order for conducting a proportionality check when deemed necessary.

11) An exemption for SMEs is required to prevent market disadvantages

Whereas many new legal instruments which concern the cooperation between law enforcement and private companies are drafted with having the main large international service providers in mind, the respective legal obligations have to be fulfilled equally by all small and medium-sized providers that still contribute substantially to the functioning of the internet eco-system. Those often do not have the necessary financial and personnel resources to comply with these obligations in the same way as a large service provider can.

ISPA Austria therefore suggests that exceptions and limitations for SMEs are to be included in the text in order to avoid that those are unproportionally affected by these new provisions. Otherwise SMEs would be placed at a clear market disadvantage vis-a-vis larger service providers that would be able to sustain such an increase in fixed costs. Such limitations could include for instance more flexible timeframes and lower fines for not being able to deliver within the prescribed timeframes.

12) Templates should be used to enhance the correspondence between LEA and ISPs

In order to accelerate 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.

13) The competent authorities in the receiving state should be notified about every cross-border order

ISPA Austria welcomes the option that the receiving party may either require notification of or consultation with their competent authorities when a provider receives a cross-border order under section 4. Such a notification would provide an important additional safeguard as also recognized in the explanatory report at para 21. Exactly since it is such an essential safeguard it is however difficult to understand, why it should be left to the discretion of each party to implement such a notification procedure.

In order to safeguard the rights of the affected individual in the context of cross-border production orders and to provide legal certainty for service providers it is indispensable that also authorities in the receiving party are involved in the process. This is necessary since it is predictable that law

enforcement agencies of the requesting party will usually prioritize their own interests over those of another state and their citizens. Without any notification of the competent authorities in the receiving party, the full responsibility of checking an order for abuse and human rights violations would rest with the service provider. ISPA Austria clearly opposes such a privatisation of law enforcement.

ISPA Austria rather insists on a mandatory notification of the competent authority in the receiving party. Although preference is given to notification already by the requesting party, also a consultation procedure as provided in 4.1.5.b could be envisaged, provided that the current limitations on 'identified circumstances' would be deleted. 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.

14) Single points of contact (SPOCs) should be used for the transmission of cross-border orders

According to the current draft, cross-border orders under section 4 could in principle be issued by any law enforcement agency which a party provides with the necessary legal competence. However, our member companies' experience clearly shows that having one single point of contact (SPOC) on the side of law enforcement facilitates and accelerates the process and adds security to both parties. In particular, service providers currently receive a large number of informal requests on technical issues prior to receiving a production order. This could be avoided to a large degree 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.

ISPA Austria thus suggests adding a provision which requires that 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.

15) User notification should be required as the default setting

ISPA Austria recognizes that as indicated in para 17 of the explanatory report to section 4 user notification is currently generally permissible where not prohibited under the domestic law in the receiving state.

User notification is a precondition to allow affected individuals to exercise their rights and apply for remedies, as they are usually unaware that their personal data has been disclosed to a law enforcement agency. Although in order to safeguard amongst others, the prevention, investigation and prosecution of criminal offences these rights can be limited, it follows from the case-law of both

the CJEU and the ECtHR that the person affected must be notified as soon as it would no longer jeopardises on-going investigations.[9]

Considering its significance ISPA Austria thus suggests that user notification should not only be permissible but rather be required as the default setting. Requiring user notification as the default setting would not only enhance transparency of state surveillance and reduce the burden of service providers but especially contribute to allowing the affected individual to exercise her procedural rights.

In case a 'gag-order' is attached to the production order it is important to clarify in the protocol that information must be added which demonstrates that the notification would jeopardise an on-going investigation or endanger the life or physical safety of an individual. In no case should the service provider become liable for not performing such verification.

16) A high level of transparency will ensure the smooth application of the suggested measures

Due to the immanent cross-border nature of the interaction between parties and service providers hitherto it has proven difficult to identify room for improvement within the cooperation as in the absence of concrete information on e.g. the total number of requests received, any suggestions for improvement will be based on anecdotal evidence and thus lack grounds for substantial improvements.

To avoid this, obligatory transparency rules including clear metrics should be added for parties and published by the Committee on an annual basis. It should furthermore also be clearly laid out that ISPs must not be banned from publishing aggregated statistics on the number of cases received.

ISPA would like to reiterate that it is very thankful for this opportunity to contribute. For further information or any questions please do not hesitate to contact us.

Sincerely,

ISPA Internet Service Providers Austria

Dr. Maximilian Schubert
Secretary General

[9] CJEU 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 para 121; *Weber and Saravia v Germany* App no. 54934/00 (ECtHR 29 June 2006) para 135; Zakharov v Russia App no 47143/06 (ECtHR 22 October 2009) para 287