EuroISPA's comments on the provisional text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime – 5th 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 new draft provisions put forward for the 5th round of consultations on the 2nd Additional Protocol to the Cybercrime Convention:

1. The need of an explicit expression of the non-binding character of requests in article 6

EuroISPA considers it important that Article 6 paragraph 1 states explicitly that the requests for domain name registration information are non-binding as is already stipulated in paragraph 6 of the explanatory remarks to Article 6 on p. 32. This is crucial, particularly considering that the explanatory remarks refer to the use of the domestic procedure to issue an 'order' – which by itself would be binding. It is foreseeable that without an explicit mentioning of the non-binding character of the request already in the text of the Article, some parties of the protocol will determine the requests binding whereas others do not, leading to a not-at-all harmonized level regarding these requests.

Recommendation: Article 6 paragraph 1 must state clearly and explicitly that the requests are non-binding. Besides, in paragraph 6 of the explanatory remarks to Article 6 it should be clarified that even if a state party chooses to use the domestic procedure to issue an 'order', such must be considered as a non-binding request in the receiving state.

2. All orders and requests to companies should be transmitted via a Single Point of Contact (SPOC):

EuroISPA already highlighted in its comments to the previous rounds of consultations the importance of having one single point of contact (SPOC) on both sides of an order or request to facilitate and accelerate the process. However, in the new draft, article 6 "Request for domain name registration information", fails again to consider this crucial aspect. According to the draft, the requests for domain name registration information could be issued by any law enforcement authority of a party which has the competency under domestic law. EuroISPA's experience shows that having a SPOC facilitates and accelerates the process and adds both legal and technical security to both parties. This positive experience has also been highlighted in Europol's Sirius EU Digital Evidence Report 2019, which shows that countries

with a SPOC in place have a higher success rate and higher level of satisfaction in cooperation with foreign service providers than such without a SPOC.[1]

Therefore, the establishment of a SPOC would alleviate many of the concerns raised in this contribution, in terms of legal certainty, trackability of the orders, security of the transmission. Furthermore, the use of this SPOC should be standardized and provide law enforcement authorities with ready-to-fill templates in order to reduce the administrative burden on the one hand, but also to allow for a technical integration on the side of the ISP and thus reduce the chances of mistakes, that would ultimately lead to longer procedures.

Recommendation: Establish the use of SPOCs as mandatory for the transmission of all cross-border orders and requests to companies, including those foreseen in Article 6.

3. The lack of prior review by a judge or other independent authority creates legal uncertainty

Article 6 leaves it to the discretion of the parties to decide which authorities can issue a cross-border request for domain name registration information. Even though EuroISPA understands that parties may have different ways of requesting data in criminal proceedings, this could lead to legal uncertainties as the entities providing domain name services – primarily registries and registrars - would have to assess the legality of the requests themselves. This uncertainty would leave most entities, in particular those without their own legal counsel, reluctant to respond to any foreign request and thus endanger the whole concept. Therefore, the prior review of such a request by a judge or another independent authority would be beneficial in many cases, and the concept should be incorporated into the protocol.

Recommendation: Introduce the mandatory prior review of cross-border requests for domain name registration information by a judge or another independent authority, in order to provide legal certainty and increase the chances of providers responding to the requests.

4. A unified model for the transmission of requests is needed

As already included in our response to the previous rounds of consultations, we believe that it is imperative to foster the use of templates for cross-border orders and requests. Templates can help accelerating the requesting process and minimize the risk of mistakes and legal uncertainty.

Such a template should specify the voluntary nature of a response to such a request, in order to avoid confusion on the side of a receiving entity and advise the company to check with their local laws if and how to respond to such a request. In particular, the reference to an international treaty such as the Budapest Convention could easily imply an obligatory nature of such a request.

Furthermore, precise specifications on language requirements are necessary, in particular, in which languages entities covered should receive such orders, in which languages they can raise questions for clarifications to the ordering authority, etc. Unfortunately, it is not clear whether the language requirements in Article 1 sub-paragraph 2 would be applicable as the wording only address direct

[1] SIRIUS EU Digital Evidence Situation Report 2019, Europol (December 2019)

disclosure, preservation and emergency disclosure. Requests under Article 6 should therefore be explicitly included as well.

Finally, in order to support the secure and efficient transmission of data requested, a data exchange system should be established, that would also serve to facilitate the authentication process and thus allow entities providing domain name services to respond more rapidly to foreign requests. Where such companies 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.

Recommendation: Develop a template for the transmission of requests which ensures that all formal requirements, including the information necessary, is included in the request. This model should also specify the voluntary nature of the response. Moreover, the language requirements in Article 1 should be extended to direct cross-border requests. Additionally, a data exchange system should be established to help companies that do not have such a system in place to streamline the requests.

5. The need for an additional legal basis for voluntary requests within EEA states must be assessed

According to Article 6 sub-paragraph 2, Parties to the Protocol shall adopt the necessary legal basis to permit an entity in its territory to disclose domain name registration information in response to a request by a foreign authority under the Protocol. For companies that fall under the scope of the GDPR, it should first be assessed to what extend the GDPR would already provide such a legal basis and if not, which other conditions such a legal basis would need to fulfill. Considering that many Parties to the Budapest Convention also are subject to the GDPR, consultation on this important aspect with the European Data Protection Board would be advised.

Recommendation: Consult the EDPB on the need for a legal basis for voluntary requests for companies that already fall under the scope of the GDPR.

6. The use of the 24/7 network should be considered as an alternative to direct cross-border orders

EuroISPA welcomes the approach the Council of Europe has taken in the draft of Article 7, to accelerate the communication between state parties by making use of the 24/7 network provided in Art 35 of the Budapest Convention which amongst others was exactly created to ensure immediate assistance in the collection of electronic evidence. The use of this network ensures not only expedited processing of data requests but at the same time legal certainty for the service provider, who receives a production order from a domestic law enforcement authority. From EuroISPA's perspective, such a system should be preferred over Article 4 ("Direct disclosure of subscriber information") which would constitute a significant renunciation from traditional forms of international cooperation and moreover bring upon a wide range of other problems which EuroISPA has already illustrated in detail in our response to the 4th round of consultations. Unfortunately, most of the concerns and suggestions raised therein have so far not been taken into account.

EuroISPA thus urges the Council of Europe to further extent the use of the 24/7 network for data requests also to non-emergency situations and exclude the controversial provision in Article 4 entirely from the

draft. Indeed, this will require additional resources to be provided by the state parties in order to have sufficient trained and equipped personnel available to handle requests. Nevertheless, it would lead to a solution that satisfies both the need for rapid cross-border access to electronic evidence while at the same time securing legal certainty and due process.

Recommendation: Establish the use of the 24/7 network for data requests as an alternative to direct cross-border orders and to non-emergency situations, therefore excluding from the draft the provision of Article 4 on the direct disclosure of subscriber information entirely.