PROPOSAL FOR A REGULATION ON EUROPEAN PRODUCTION AND PRESERVATION ORDERS FOR ELECTRONIC EVIDENCE IN CRIMINAL MATTERS

EuroISPA's considerations **June 2018**

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. EuroISPA has long been engaged on the e-evidence file, having been very active in the proposal's preparatory stages.

As discussions develop in the EU Institutions, EuroISPA hereby sets out its position on the e-evidence proposal:

The inclusion of cost reimbursement is welcomed as a positive step, but as it remains a national prerogative, it cannot be used EU-wide as a potential tool to disincentivise judicial authorities from issuing bad faith or frivolous Orders. For example, a nominal fee per Production Order could also serve as a check on the volume of Orders sent out.

A. We criticise the further privatisation of law enforcement by this proposal

- The e-evidence proposal, through the proposed pan-European ISP-judicial authority cooperation, entails that ISPs are expected to place **a high level of trust** in all 28 Member States' legal systems. However, legal uncertainty is caused for ISPs as a result of any national judicial authority across the EU being enabled to send a Production Order to ISPs in any jurisdiction. ISPs are accustomed to cooperating with domestic judicial authorities and have effective and fruitful cooperation on the national level.
- We notice some lack of clarity around the information made available to companies assuring them that requests comply with laws on the grounds of 'necessity and proportionality'. However, we strongly advocate for service providers not to become the actors responsible for checking Orders against the local or the requesting Member States' law and signal non-compliant or abusive Orders. We are of the strong belief that this is a task for judicial authorities in the two countries involved – not only because SMEs in particular do not have the legal capacity to perform this review. Nevertheless, the inclusion of further information in the Order (e.g. a clear subject, a clear sender, a clear mention of the law being infringed, etc.) would be necessary for providers to comply with the procedure as mentioned in Art. 9 (5).

- The **conflict of law** remedies are, in practice, expected to be inefficient and also pose a threat to due process as well as to the rule of law as a result of the unfeasible deadlines set out by the proposal. For example, service providers are obliged to respect a six-hour deadline to comply with orders in emergency cases, which are clearly unpracticable where questions of a conflict of law become apparent.
- In the context conflicts of law with third countries, we encourage policymakers to set up the framework in the e-evidence proposal to negotiate international cooperation agreements to provide legal certainty.

B. There is cause for concern over the legislative asymmetries amongst Member States

- Clarity is needed regarding **principles of double criminality** for both Member States involved. Further provisions should be included to establish whether similar legal grounds are required between the two Member States involved to proceed with issuing and executing a Production Order. This would serve to ensure legal clarity for ISPs in complying with Production Orders.
- **There exists a significant disparity across Member States for crimes entailing a three-year sentence**. This threshold, chosen for issuing Production Orders for transaction or content data causes legal uncertainty for service providers, where the criminal investigation in which they are expected to cooperate can vary significantly from Member State to Member State. As a result, the threshold should be raised to e.g. five years or the applicability should be restricted to an exhaustive list of criminal offences (which is already the case for the EIO).

C. The proposal is lacking in provisions and adaptability for SMEs

- **Timeframes** in the e-evidence proposal for the execution of Production and Preservation Orders are not feasible for SMEs, who mostly do not run 24/7 services. This is especially problematic for emergency cases, where a six-hour time frame is simply not practicable for a grand majority of EuroISPA's membership.
- **SME exemptions** should therefore be included to offset the greater administrative burden incurred by the proposed cooperation mechanism. SMEs would be placed at a clear market disadvantage, causing competitiveness issues, where only larger service providers would be able to sustain such an increase in fixed costs.
  In case SMEs are not excluded, they should at least not be subject to equal fines for not being able to deliver within the prescribed periods. Furthermore, separate and more practical time-periods for SMEs should be provided.

D. Clearer safeguards in Order authentication processes should be included

- Current provisions for the **authentication of Order Certificates** are insufficient. It is impossible for ISPs across the EU to verify the authenticity of each national judicial authorities' stamp and signature. Therefore, a more robust verification system is absolutely necessary. Conditions for the **security and integrity of data transfers** in executing a Production Order should be included in the cooperation framework, as already provided for in some national systems.
- In some countries (e.g. Austria) technical systems for secure data provisioning between ISPs and LEAs are already well established and also serve as a verification mechanism. They have improved the communication between ISPs and LEAs significantly. In order to make the e-evidence proposal workable in practice, a similar EU-wide system should be put in place, which would

safeguard data protection and due process in cooperating in criminal investigations while at the same time allow for quick data transfers when necessary.

- There is a **lack of a clear threshold for judicial authorities issuing Production Orders to prove that the criteria for issuing an order are fulfilled.** Independent oversight should guarantee the respect of **principles of proportionality and necessity.** However, many ISPs are generally not in the position to conduct such an assessment, thus this legal guarantee should be provided by national courts.
- The EU-US MLAT is an example where criteria are set out for judicial authorities in order to prove that the threshold is met for sending data requests to service providers. These stipulations consist of the requirement of reasonable suspicion of the data subject's involvement in criminal offence as well as the provider's likely possession of the relevant information.

E. There is the risk of fragmentation due to data categorisation in the e-evidence proposal, notably for metadata

- According to the proposed definitions, metadata falls in both the categories of access and transactional data. This causes issues due to the discrepancy in data categorisation set out by the ePrivacy proposal, raising questions as to the interaction of the two proposals.
- The categorisation of types of metadata also means that companies incur a greater burden and costs in their own compliance processes. Mechanisms will need to be implemented so as to treat access and transaction data differently, to ensure service providers are able to comply with Production Orders.
- A harmonisation of data categories across EU legislation would provide legal certainty and a more cost-effective approach for internal ISPs' internal compliance mechanisms.

F. There should be a greater coherence with international standards for data transfer requests

- The cooperation framework as set by the e-evidence proposal should be more workable with regards to international standards, for example those included in the Budapest Convention.

G. Member States should publish statistics for the purpose of transparency

- Although the proposal already requires Member States to provide comprehensive statistics on Production and Preservation Orders issued by relevant authorities, there is no provision which would secure the enforcement of this obligation. Statistics of the receipt and sending of Production and Preservation Orders however are key for transparency in the cooperation between service providers and judicial authorities. The Commission should be in a position to enforce such measures.
- No confidentiality clause introduced by the proposal should prevent ISPs from publishing voluntary transparency reports.

H. Clear safeguards on the protection of encrypted data should be included

- According to Recital 19 of the proposal, data must be provided regardless of whether it is encrypted or not. However, clear safeguards on the protection of encrypted data should be included in the proposal as well as a clarification that ISPs will not be responsible for its decryption in any way. By handing over such data to an authority, ISPs might be forced to

involuntarily transmit more data than necessary to judicial authorities. This includes potentially confidential data protected by the law, such as data pertaining protected professions (e.g. lawyers, doctors, etc.).

I. Conclusion

EuroISPA has been a longstanding interlocuter in policy discussions on how to improve cooperation procedures, using its representative role at, for example, Europol's EC3 communications providers advisory group, the European Commission DG JUST/DG HOME taskforce on e-evidence, and the former European Commission expert group on data retention, to advance such discussions.

EuroISPA and its members feel compelled to stress the negative consequences that will arise from any framework that privatises law enforcement and does not provide clear safeguards for ISPs. Furthermore, EuroISPA emphasises the need for SME exemptions to offset the considerable administrative, legal and financial burden incurred by the cooperation set out by the e-evidence proposal.