European Commission
DG for Justice and Consumers
1049 Bruxelles/Brussel
Belgium

Vienna, 18th July 2018

ISPA CONTRIBUTION TO THE PUBLIC CONSULTATION ON THE PROPOSAL FOR A REGULATION ON EUROPEAN PRODUCTION ORDERS FOR ELECTRONIC EVIDENCE

Dear Sir/Madame,

ISPA (Internet Service Providers Austria; Identification Number: 56028372438-43) is pleased that the European Commission has issued this public consultation on the Proposal for a Regulation on European Production Orders for electronic evidence and would like to share its position on this important subject.

ISPA considers the inclusion of cost reimbursement in the proposal 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 serve as a check on the volume of orders sent out.

ISPA feels compelled to request that national authorities in the receiving state need to be under the obligation to assess the necessity as well as the proportionality of any incoming Order and stresses the negative consequences that will arise from any framework that privatises law enforcement and does not provide clear safeguards for ISPs. Furthermore, ISPA emphasises the need for SME exemptions to offset the considerable administrative, legal and financial burden incurred by the cooperation and the extremely ambitious timeframes suggested by the e-evidence proposal. In detail ISPA would like to draw the European legislator's attention notably to the following issues:

1. ISPA strongly opposes 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 an extraordinary high level of trust in all 28 Member States' legal systems. This causes significant legal uncertainty for ISPs due to 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.

ISPA notices a lack of clarity regarding 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 as well as to signal non-compliant or abusive Orders. We strongly believe that this is a task for judicial authorities in the both countries involved – notably because SMEs in particular do not have the legal capacity to perform this review.

In ISPA's opinion the judicial authorities of the Member States should be strictly obliged to review the Orders against the local or the requesting Member States' law, which also would guarantee a minimal degree of sovereignty being retained by the receiving state.

The majority of the ISPA's members consists of small and medium-sized ISPs, which are not equipped to deal with such complex legal matters and especially those companies should be considered within the revision of the proposal.

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 is, in practice, expected to be inefficient and also pose a threat to fundamental principle of due process as well as to the rule of law as a result of the absolutely unfeasible deadlines set out by the proposal. For example, service providers would be 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 this respect, ISPA also objects against any kind of fast track procedures for emergencies, due to the bad experience with law enforcement authorities abusing such procedures in the past. In case that such fast track procedure would be still foreseen, it must be bound to significant monetary expenses for the requesting authority, to prevent the abuse of such expedited requests. Such fast track procedures not only put tremendous pressure onto ISPs, which will be obliged within extremely short timeframe to provide excellent quality responses, but also lowers the standards of due process and rule of law.

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.

2. ISPA is concerned over the legislative asymmetries amongst Member States

In ISPA's opinion, 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 (as is already the case for the EIO).

3. ISPA underscores that 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 under no circumstances 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 ISPA'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.

4. 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. The current provisions not only undermine the high level of security standards already established in the telecoms and internet sector, but they also might lead to abuse of the system, which would thereby also lower the trust of users in ICT infrastructure and would impede the digitalisation of the European economy.

Therefore, a very 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 Austria a very well proven and generally widely accepted technical system for secure data transfer between ISPs and LEAs has already been well established and due to its low implementation and running costs (requires only a browser application at the client side while

providing transparency as well as a high level of security through multiple layers of encryption) could serve as a blue print for a verification mechanism. The system also contributed significantly to the improvement of the communication between ISPs and LEAs in Austria.

In order to make the e-evidence proposal workable in practice, a similar EU-wide system would need to 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 and secure data transfers when necessary.

There is also 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.

5. The risk of fragmentation due to data categorisation in the e-evidence proposal, notably for metadata should be properly addressed

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.

By Austrian standards the proposal would mean that traffic data (e.g. IP addresses) would fall into the section of "access" data and thereby would receive a lower level of protection. This provision is in clear contradiction with the judicial decisions on traffic data, therefore ISPA objects strongly against this lowering of the protection standards, as only data that can be provided without the processing of traffic data should be deemed "access data"[1].

The different 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.

[1] § 92 Abs. 3 Z 16 iVm § 99 Austrian Telecommunications Act; OGH, 4Ob41/09x v. 14.07.2009 *LSG gg. Tele2*.

6. **A greater coherence with international standards for data transfer requests should be applied**

In ISPA's opinion the cooperation framework as laid out by the e-evidence proposal should be more workable with regards to international standards, for example those included in the Budapest Convention.

7. **Member States should publish statistics for purposes 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. In this respect, ISPA would like to point out that the Commission had failed in previous cases to receive statistics from member states (e.g. data retention directive) and therefore sees an immanent need to avoid similar failures in the future.

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 therefore needs to be in a position to enforce such measures and might be well advised to opt for a technical implementation (e.g. Austrian DLS) which already provides reporting and transparency features ('transparency by design').

No confidentiality clause introduced by the proposal should prevent ISPs from publishing voluntary transparency reports.

8. **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 under no circumstances be responsible for its decryption, in any way. ISPA furthermore would like to point out that by handing over encrypted 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 to protected professions (e.g. lawyers, doctors, etc.).

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
General Secretary

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675

About ISPA: ISPA is the Austrian association of Internet Service Providers, representing approximately 220 ISPs. ISPA is a major voice of the Austrian Internet industry. Our goal is to shape the economic and legal framework to support optimal growth of the Internet and Internet services. We regard the use of the Internet as an important cultural skill and acknowledge the resulting socio-political responsibilities.

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675