Position Paper on Data Retention

EuroISPA acknowledges the challenge of granting adequate means to law enforcement authorities (LEAs) to prevent and prosecute serious crimes, while safeguarding the fundamental rights of users and electronic communications services (ECS) providers. In light of the current discussions within the High-Level Group on access to data for effective law enforcement, EuroISPA developed a list of imperative requirements to provide guidance on how to achieve the right balance between the interests and obligations of all parties involved. All while respecting the jurisprudence of the CJEU that has clarified that such rules should not create obligations for ECS providers to store additional user data than what is necessary for legitimate purposes.

Imperative Requirements

1. **Legal certainty:** Any type of consideration for a new data retention regime or, in general, for provisions for requiring the storing data emanating from ECS, must draw their limits in the jurisprudence of the European Court of Human Rights (ECtHR) and CJEU case law, that have already clarified the confinements and tight requirements under which the collection of data could be legitimate. In particular, it should be clear under which circumstances electronic communications services (ECS) providers can be required to retain specific users' data with the ultimate aim of granting LEAs access to it. In addition, harmonisation with the *acquis communautaire* should be ensured.

2. **Scope of the legal framework:** Any new EU data retention legal framework should be limited to basic subscriber information and traffic data and exclude content data. Already the CJEU has clarified in *Digital Rights Ireland*, that retention of content data would adversely affect the essence of the fundamental right to privacy and thus be unlawful.

3. **Harmonisation:** Any new EU data retention framework should aim to harmonise among Member States the data categories concerned, the maximum data retention periods, the definition of serious crimes for which such data can be retained, and data protection requirements. Inconsistencies or excessive requirements would increase burdens and costly inefficiencies. This is particularly relevant in view of the cross-border and globally distributed nature of number independent interpersonal communication services (NI-ICS).

4. **Clear conditions for targeted data retention**: Any future EU legislation must provide clear objective criteria to define the specific circumstances and conditions under which a service provider in scope must retain individual users' data for the purpose of granting access to LEAs. These conditions must ensure – in line with the clear requirements set by the CJEU – that the data categories retained, the people affected, and the retention times are limited to what is strictly necessary for the prosecution

EuroISPA
Rue de la Loi 38, 1000 Brussels
secretariat@euroispa.org
EU Transparency Register: 54437813115-56

of serious crimes. Data retention obligations can at utmost be imposed in relation to the prosecution of the serious crime and to the benefit of clearly (exhaustively) articulated competent authorities.

5. **Categories of data to be retained:** The list of data categories that have to be retained on a mandatory basis should be proportionate, i.e. only data already processed and stored for billing, commercial, technical, security or other legitimate purposes. The conditions for ordering the retention of data should vary according to the data category concerned.

6. **General conditions for LEA access to retained data:** While the legal procedure under which a provider in scope must disclose data to national LEAs should comply with applicable laws, including the e-Evidence Regulation, it must be ensured that access by LEAs to such data is strictly limited for the purpose for which it was retained (the prosecution of serious crimes) and, that only data retained of individuals involved in committing or planning a serious crime is being disclosed. Furthermore, cross-border preservation and production orders should continue to be exclusively regulated under the e-Evidence framework.

7. **No direct access to retained data**: To ensure the security, privacy and integrity of networks, all access demands must be implemented solely by the relevant ECS provider upon receipt of appropriate legal documentation (in relation to which service providers should be granted an opportunity to object to or challenge the order). Member States should not be permitted to require installation of government equipment within privately operated networks.

8. **Definition of "serious crime" in national law:** Definitions should be orientated in line with the scope of applicability of the European Arrest Warrant and the E-Evidence Regulation. This serves as harmonisation regarding the protection of fundamental rights by the EUCFR. A clear definition of "serious crime" in any future legislation on data retention will further provide legal certainty among Member States in the course of the implementation. This will contribute to limiting the retention of data to what is strictly necessary and proportionate, avoiding abuse and allowing a better coordination of cross-border law enforcement investigations.

9. **Ensuring independent oversight by a judicial authority:** Any national order to retain data must be subject to prior review by a judicial authority from the country of establishment of the ECS provider.

10. **Data localisation:** The cross-border movement of data is critical to the development and growth of the EU and should not be limited by localisation requirements, which disproportionately impact cross-border services. In case a data localisation requirement is stipulated, it should be done in line with the EU's Free Flow of Non-Personal Data Regulation, meaning national-specific storage, security and retrieval measures should be prohibited, as these cause huge inefficiencies in time and cost. Instead, this should be done at the EU level in line with single market principles. Moreover, an important share of the interpersonal communication services are globally distributed and cross-border. To reflect the nature of those services, providers must be permitted to address lawful intercept requirements from their place of main establishment in the EU and should not be required to maintain infrastructure or personnel in any member state other than or in addition to that of their main establishment for the sole purpose of facilitation of law enforcement access demands.

11. **Retention period:** Data should be retained only for the period which is necessary for the prosecution of a serious crime. In order to provide legal clarity andcoherence with the jurisprudence of the CJEU, any legislative proposal should determine a maximum retention period. By using an opening clause, Member States should however be free to define a lower data retention period where found to be sufficient. In general, no minimum retention period should be stipulated, as the purpose of any new regime would not be to require retention across Europe, but to regulate it where it exists so as to comply with European standards and fundamental principles of law.

12. **Mandatory cost-reimbursement:** Ensuring compliance with data retention legislation creates high costs to develop and maintain the provider's internal systems. Indeed, ECS providers face enormous data retention costs due to necessary adjustments to their network systems, investments in data storage and IT security, technology, as well as IT systems to translate and process massive amounts of data into useful retrievable information for law enforcement purposes. Any new data retention rules should therefore include mandatory cost-reimbursement provisions (investment and retrieval costs) and not leave it to the discretion of Member States. Such a provision will also act as a safeguard against excessive requests. Good practices, such as the Finnish model,[1] should be encouraged across the EU.

13. **Flexibility of processes:** ECS Providers must be able to store the data securely and organise this process in the most efficient and effective way to their operations.

14. **Single point of contact with the LEA:** In order to maintain consistency and efficiency, a single LEA within a given Member State should be identified to contact the ECS provider, rather than a variety of authorities.

15. **Capabilities of SMEs and specificities of B2B providers must be taken into account following the proportionality principle:** Exceptions and limitations should be included for SMEs and companies that receive a low number of data requests by LEAs, such as B2B providers, as the burden for these companies and infringement in their freedom to conduct a business would be disproportionate to the benefit in the fight against serious crime. In this respect, the particularities of business customers should be taken into account, since the retention of data of one customer would lead to the retention of data of up to thousands of individual employees, which would also be disproportionate.

16. **User notification:** Users whose data has been retained should be notified by the competent authority about this action unless notice would jeopardize on-going investigations. Voluntary user notifications by the ECS provider should only be prohibited where duly justified by the competent authority.

17. **Secure transmission of data:** Where service providers, Member States or Union bodies have established dedicated platforms or other secure channels for the handling of data these should be used by LEAs and judicial authorities.

[1] The cost reimbursement is based on Section 299 (1003/2018) of the Finnish Act on Electronic Communications Services, "Costs incurred by systems acquired for assisting public authorities", whereby "A telecommunications operator has the right to receive compensation from State funds for the direct costs of the investment and maintenance of systems, equipment and software acquired for the sole purpose of assisting public authorities. […]"

18. **Transparency:** As already included in the former Data Retention Directive, Member States should be obliged to provide statistics on the use of retained data for law enforcement in order to be able to provide substantial evidence for a further improvement of the system.

19. **Evaluation:** As data retention constitutes a substantial infringement to the privacy of end-users and to the freedom to conduct a business, an evaluation of potential data retention regulations should occur every two years.

About EuroISPA

Established in 1997, EuroISPA is the world's largest association of Internet Services Providers Associations, representing over 3,300 Internet Service Providers (ISPs) across the EU and EFTA countries. EuroISPA is recognised as the voice of the EU ISP industry, reflecting the views of ISPs of all sizes from across its member base.

EuroISPA
Rue de la Loi 38, 1000 Brussels
secretariat@euroispa.org
EU Transparency Register: 54437813115-56