EuroISPA Letter to the European Commission on e-Evidence

June 2025

EuroISPA thanks the European Commission for the continued engagement and consultation with Internet Services Providers (ISPs) on the implementation of the e-Evidence Regulation and Directive. However, EuroISPA wishes to share some key concerns, open questions and requests for clarification in anticipation of the upcoming implementing acts and the operationalisation of the decentralised IT system.

1. Legal scope and applicability

There remains substantial uncertainty regarding the interaction between the Regulation and the Directive, in particular:

- The scope of application for services providers offering services exclusively within one Member State. Does Article 1(5) of the Directive exclude these actors from both instruments? What is the Commission's view on the specific criteria for a service provider to qualify for the exception, and how can individual cases be assessed—for example, company groups where each entity offers services in only one Member State? Given the strict penalties for non-compliance, it is especially important for smaller service providers to have legal certainty as to whether they fall within the scope of the e-evidence regime.

We respectfully request clear and consolidated guidance on the delineation of obligations for such cases.

2. Technical framework and security concerns

Several critical issues remain unresolved in relation to the decentralised IT system:

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

- **Absence of E2EE**: the current draft of the implementing act leaves the decision to require end-to-end encryption (E2EE) to the discretion of the Issuing Authority, which raises serious concerns given the highly sensitive nature of the data being exchanged. We strongly advocate for mandatory, full E2EE from originator to recipient to drastically reduce attack surfaces and protect the integrity and confidentiality of sensitive legal data requests.
- **Authentication of Issuing Authorities**: there is currently no defined process to authenticate the legitimacy of Issuing Authorities beyond their access to e-Codex, potentially exposing the system to misuse or phishing attacks by bad actors.
- **Service provider specific inputs**: to improve the accuracy and efficiency of the DIS, it is essential that the Commission's Reference Implementation (RI) include an opt-in feature allowing large service providers to directly populate specific fields. This would enhance the clarity and consistency of requests.
- **Streamlining Request Creation**: specifically, we propose that large providers be able to: (i) supply values for the "target identifier" dropdown in Section E of the EPOC form – allowing requesters to select from a provider-verified list of identifiers (e.g. "email", "username"); and (ii) populate the data category checkboxes in Section F – enabling requesters to choose only those categories relevant to the provider's actual services.
- **Benefits of Provider-Specific Inputs**: this approach would: (i) improve clarity and consistency by relying on provider-verified information; (ii) increase transparency for both requesters and service providers regarding the data requested; (iii) streamline the process and minimise errors by helping requesters quickly select accurate identifiers and data categories. Importantly, this proposal emphasises that requesters would still retain flexibility via an "Other" option and free-text field, ensuring the system remains adaptable.

We strongly encourage the Commission to determine standardised, secure processes in the case that data exchange over the decentralised IT system is not possible.

We emphasise the importance from an efficiency and cost saving perspective, to integrate the existing local platform solutions for collaboration (e.g. TANK in Belgium) with the decentralised IT platform.

3. Implementation timelines and transition period

EuroISPA urgently calls attention to the severe and unaddressed challenges jeopardising the timely implementation of the DIS. Our members' concerns stem from critical issues that, if not immediately rectified, will inevitably lead to significant delays and operation disruption.

- **Resource demands**: the significant technical and human resource effort required on the service provider's side to connect to the decentralised system, which may range from a few months (if integrating existing infrastructure) to over two years (if building new systems).
- **Regulatory ambiguity**: the lack of clarity surrounding the operational transition between the publication of the Implementing Act and full deployment, particularly given Article 24 of the Regulation, creates a dangerous vacuum of information, leaving stakeholders in limbo and unable to plan effectively. Without a defined roadmap, the path to full deployment is fraught with uncertainty.

- **Lack of preparatory guidance**: the absence of clear criteria, documentation, or testing protocols prevents meaningful preparation, leaving service providers ill-equipped for complex integration.

We urge the Commission to provide a realistic roadmap, allow sufficient lead time, and facilitate early technical engagement with services providers and national authorities.

4. Remuneration and cost reimbursement

We ask clarity on:

- Whether existing national systems can be maintained or integrated with the EU framework.
- How will the Commission ensure that the remuneration framework for compliance costs is transparent and easily accessible, allowing service providers to submit remuneration requests without the need for extensive research into foreign legal systems?

Clear, harmonised principles for cost recovery would ensure fair implementation across the internal market.

In addition to covering ongoing compliance costs, the framework should also address the initial costs of implementation, which will be substantial. Furthermore, there must be clear provisions on enforcement: what recourse will providers have if a foreign authority fails to pay its due costs?

5. Anticipated Request Volume and Operational Load

Current estimates for the volume of preservation and production order that will be issued to service providers under the Regulation vary significantly (e.g. 200-300 to 100,000+ per provider per year), yet there is a complete absence of formal forecasting or a proper impact assessment. Services providers are concerned about:

- **Unpredictable workloads**: the absence of reliable data creates a perilous environment, especially if the Regulation dramatically increases cross-border requests.
- **Risk of unmanageable spikes**: if the DIS becomes the default for law enforcement cooperation throughout the EU, there's a serious risk of overwhelming the system, and causing systemic failures.

We recommend the Commission conducts or publishes data-driven forecasts and maintain continuous dialogue with national authorities and ISPs to prepare for operational realities.

6. Safeguards and Fundamental Rights

We reiterate the importance of preserving high standards of fundamental rights protections, including:

- Clear guarantees during the transition phase, especially when systems and safeguards may only be partially deployed.

- Implementing measures to prevent permanent reliance on “emergency” pathways or fallback mechanisms, which can lead to a long-term weakening of fundamental rights.
- Adherence to procedural clarity, data minimisation, and full transparency in line with the Charter of Fundamental Rights and applicable data protection laws, such as the GDPR.

To conclude, we appreciate the European Commission’s willingness to engage with private stakeholders and experts. To support an efficient and rights-respecting rollout of the e-Evidence framework, we remain committed to collaboration and to sharing input from our members’ national-level discussions.

We would welcome the opportunity to meet or consult further as the implementing acts are finalised.

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