2026 E-Evidence Workshop at Nordic Domain Days in Stockholm

When Abuse Meets Evidence: Preparing DNS Providers for the EU's New Reality

---

• **Date & Time:** 26 May 2026, 13:30–17:00 CEST

• **Organizer:** eco's topDNS Initiative & iQ Global

• **Target Audience:** Domain name registries, registrars, hosting providers, cloud providers, DNS operators, legal teams, compliance specialists, cybersecurity experts, and other stakeholders in the Internet infrastructure ecosystem.

Executive Summary

The 2026 E-Evidence Workshop at Nordic Domain Days in Stockholm, hosted by eco's topDNS Initiative and iQ Global, examined one of the most significant regulatory developments currently facing the European domain name, hosting and digital infrastructure community: the EU E-Evidence framework.

Under the title **"When Abuse Meets Evidence: Preparing DNS Providers for the EU's New Reality"**, the workshop explored what will happen when DNS abuse response, electronic evidence requests and cross-border criminal investigations begin to intersect more directly. The topic was particularly timely because the EU E-Evidence Regulation becomes applicable on **18 August 2026**, introducing new obligations for service providers to respond to European Production Orders and European Preservation Orders.

The session was opened by **Lars Steffen**, Head of International, Digital Infrastructures & Resilience at eco – Association of the Internet Industry, and **Lars "LG" Forsberg**, CTO of iQ Global. Steffen placed the workshop within the broader work of eco's topDNS Initiative, which brings together registries, registrars, hosting providers, cloud operators and other infrastructure actors to strengthen cooperation on DNS abuse mitigation, data sharing and regulatory preparedness.

The workshop featured expert contributions from **Tania Schröter**, Deputy Head of Unit at DG JUST, European Commission; **Annika Bergstedt**, Legal Adviser at the Swedish Ministry of Justice; **Thomas Rickert**, Director Names & Numbers at eco; and **Ulrich Plate**, Head of eco's KRITIS Working Group. Together, they provided a comprehensive picture of the E-Evidence framework, from the legal

architecture and Swedish implementation to technical readiness and the broader compliance burden facing digital service providers.

A central message emerged throughout the afternoon: E-Evidence is not merely a new legal instrument. It reflects a broader shift in which private infrastructure providers are becoming direct participants in cross-border criminal investigations. Under traditional mutual legal assistance mechanisms, authorities usually cooperated through government-to-government channels. Under E-Evidence, competent authorities in one EU Member State may address certain requests directly to a service provider's designated establishment or legal representative in another Member State.

For the domain name industry, this is highly relevant. The framework explicitly covers Internet domain name services and IP numbering services. Registries, registrars, privacy and proxy providers, hosting companies and other digital infrastructure operators cannot assume that E-Evidence is a matter only for major platforms or cloud providers.

The workshop also showed that legal readiness and operational readiness are not the same. The Regulation may become applicable on a fixed date, but providers still need processes for intake, verification, escalation, preservation, production, documentation and confidentiality. In standard cases, production orders must generally be answered within ten days. In emergency cases, providers may have only eight hours.

Speakers repeatedly emphasized that E-Evidence arrives within an already complex regulatory environment. Providers must also navigate GDPR, NIS 2, national disclosure rules, ICANN's Registration Data Policy, the Budapest Convention, Digital Services Act reporting obligations, and increasing requests from law enforcement, regulators and rights holders.

The workshop concluded with a practical message: preparation must begin before the first order arrives. Providers should assess whether they are in scope, designate appropriate establishments or legal representatives, build internal workflows, train legal and technical teams, and monitor national implementation developments. By Nordic Domain Days 2027, E-Evidence will no longer be an upcoming obligation; it will be part of the operational reality for digital service providers in Europe.

Introduction

On 26 May 2026, eco's topDNS Initiative and iQ Global convened an afternoon workshop at Nordic Domain Days in Stockholm to address one of the most consequential regulatory developments now facing Internet infrastructure providers: the EU's E-Evidence framework, which consists of the e-Evidence regulation (EU 23/1543) and an associated directive (EU 23/1544).

The workshop was introduced by **Lars Steffen**, Head of International, Digital Infrastructures & Resilience, eco – Association of the Internet Industry, who welcomed participants and explained that the topDNS Initiative continues to bring together different parts of the Internet infrastructure

ecosystem. Its work is not limited to registries and registrars, but also includes hosting providers, cloud services, DNS operators and other actors involved in abuse mitigation and resilience.

Steffen emphasized that the E-Evidence Regulation is highly relevant to the same community that has been working on DNS abuse, because abuse cases often generate the evidence requests that providers may soon have to process under the new framework.

The workshop was hosted and moderated by the following colleagues:

- **Lars "LG" Forsberg,** CTO, iQ Global
- **Thomas Rickert**, Director Names & Numbers, eco – Association of the Internet Industry
- **Ulrich Plate,** Head of KRITIS working group, eco – Association of the Internet Industry

The expert speakers were:

Speaker	**Organization**
Tania Schröter	Deputy Head of Unit, DG. JUST, European Commission
Annika Bergstedt	Legal Adviser, Swedish Ministry of Justice
Thomas Rickert	Director Names & Numbers, eco – Association of the Internet Industry
Ulrich Plate	Head of KRITIS Working Group, eco – Association of the Internet Industry

The workshop moved from policy to implementation and then to practice. **Tania Schröter** introduced the EU framework. **Annika Bergstedt** explained Sweden's implementation. **Thomas Rickert** connected E-Evidence to DNS abuse and provider workflows. **Ulrich Plate** demonstrated the technical and organizational challenges involved in making the system actually work. What emerged was a clear message: the deadline is close, the framework is real, and preparation cannot be deferred.

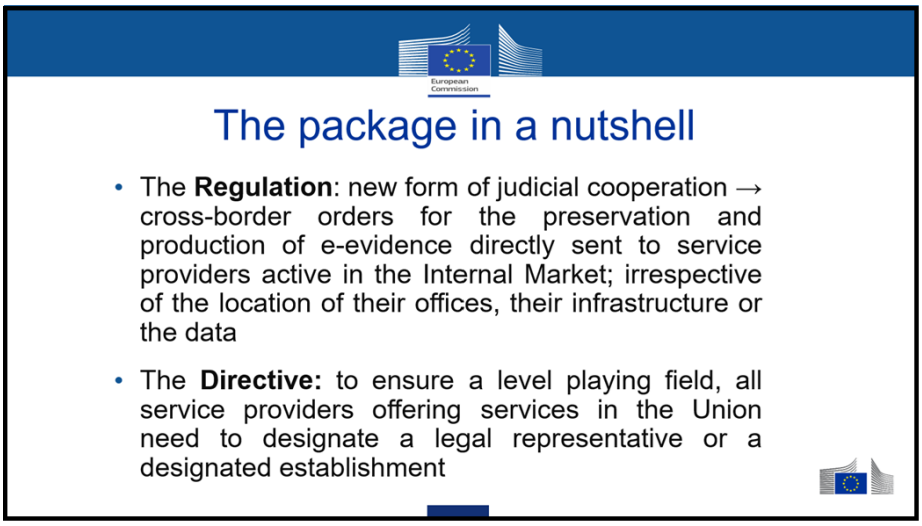
A New Model for Accessing Electronic Evidence

Opening the substantive part of the workshop, **Tania Schröter** from the European Commission explained the policy objectives driving the E-Evidence package and why it represents a genuine departure from traditional judicial cooperation.

Schröter explained that electronic evidence now plays a central role in criminal investigations. Whether authorities are investigating fraud, cybercrime, phishing, malware, terrorism or child sexual abuse material, relevant data is often held by private service providers and may be located, processed or controlled across multiple countries. Traditional mutual legal assistance procedures were designed for a more territorial environment, typically involving authority-to-authority cooperation through multiple layers of government communication. In the digital environment, where data may be volatile and investigations time-sensitive, these procedures are often too slow.

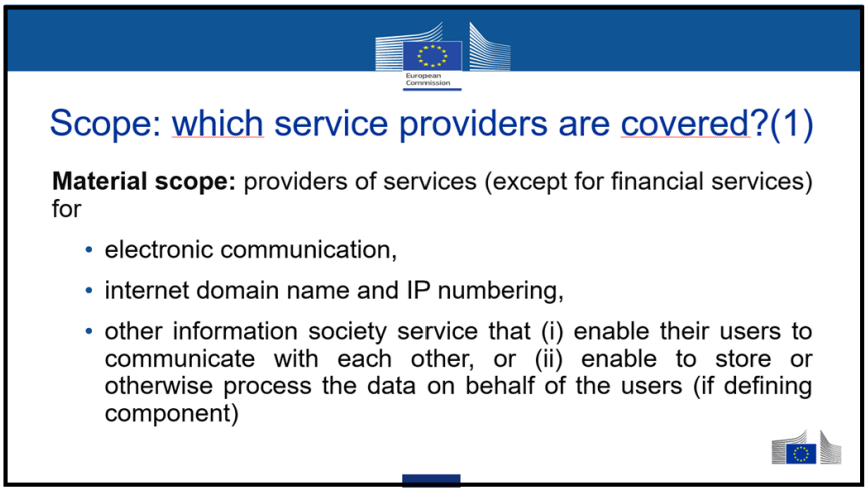
The E-Evidence framework addresses this by allowing competent authorities in one Member State to issue certain orders directly to service providers — or more precisely, to their designated legal representatives or establishments — in another Member State. This is the framework's most important innovation. Rather than routing requests through several layers of government-to-government communication, the new system creates a direct channel between the issuing authority and the provider's designated point of contact.

Schröter explained that the E-Evidence package consists of two instruments. The Regulation creates the mechanism for European Production Orders (EPOCs) and European Preservation Orders (EPOC-PRs). The Directive requires service providers offering services in the EU to designate either a legal representative or a designated establishment capable of receiving and responding to such orders.



The physical location of the data is largely irrelevant under the framework. The Regulation is designed to operate regardless of where the provider's infrastructure or data storage is located, provided the provider offers services in the Union and falls within scope. **Schröter** also noted that the framework was specifically designed to capture non-European providers that serve large numbers of EU users but may have no formal establishment here. By requiring them to nominate a legal representative within the Union, the framework ensures that all orders remain an EU-internal process.

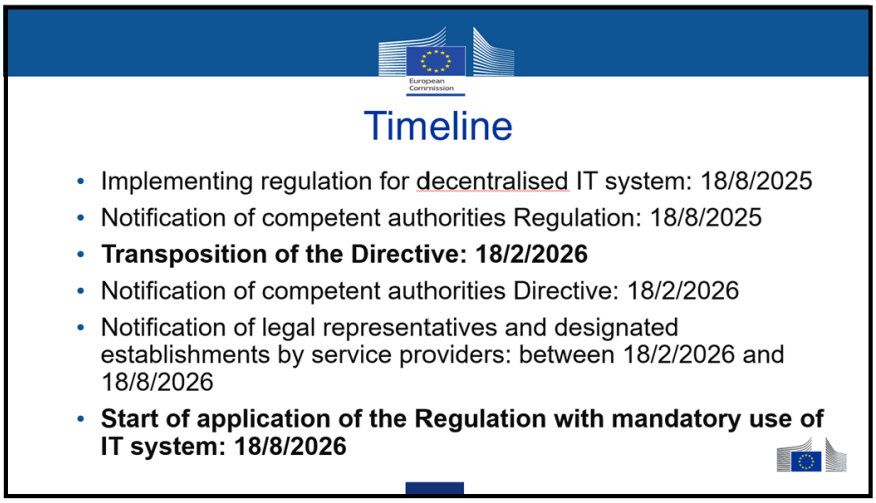
The scope is deliberately broad. It covers electronic communications providers, Internet domain name and IP numbering services, and certain information society services. This is particularly relevant for the Nordic Domain Days audience, as domain name registries, registrars, and related providers are not peripheral to the framework — they are expressly within its scope.



Schröter outlined the safeguards built into the system. Judicial authorities are involved at the issuing stage. For subscriber and user-identification data, prosecutors may be competent to issue orders. For traffic and content data, a judge or court is required. In cases involving traffic and content data, the enforcing state is also notified in parallel and may raise refusal grounds within ten days. The available grounds for refusal are deliberately narrow — covering privileges and immunities, fundamental rights in limited circumstances, double criminality, and conflicts with third-country law — and are intended to apply only rarely in practice.

Schröter stressed that the framework aims to increase speed while maintaining proportionality, necessity and procedural protections.

Schröter closed her overview by addressing the implementation timeline. The Directive's transposition deadline was 18 February 2026. The Regulation becomes applicable on 18 August 2026. However, many Member States are significantly behind schedule on both legislative transposition and technical readiness. The practical consequence is that the framework is unlikely to launch with a single harmonised “Big Bang.” Instead, implementation will be gradual, with Member States, authorities and providers connecting to the system progressively over the months that follow.



International Challenges and the US Dimension

During the discussion, participants raised questions about the relationship between the E-Evidence framework and US law, particularly the CLOUD Act and the Stored Communications Act. **Tania Schröter** explained that negotiations between the European Union and the United States on a dedicated E-Evidence agreement had progressed significantly but are currently on hold following the change of administration in Washington.

The original objective of the negotiations was to address conflicts of law that may arise when providers subject to US legislation receive requests for content data from European authorities. While the E-Evidence framework includes mechanisms for addressing such conflicts, it does not eliminate them entirely. Instead, courts may be required to balance competing legal obligations on a case-by-case basis.

Schröter nevertheless noted that many major providers have increasingly structured their European operations through EU-based entities and infrastructure, which may reduce the practical impact of such conflicts in certain situations. The issue remains relevant for providers operating across multiple jurisdictions and illustrates the broader challenge of applying territorial legal frameworks to global digital services.

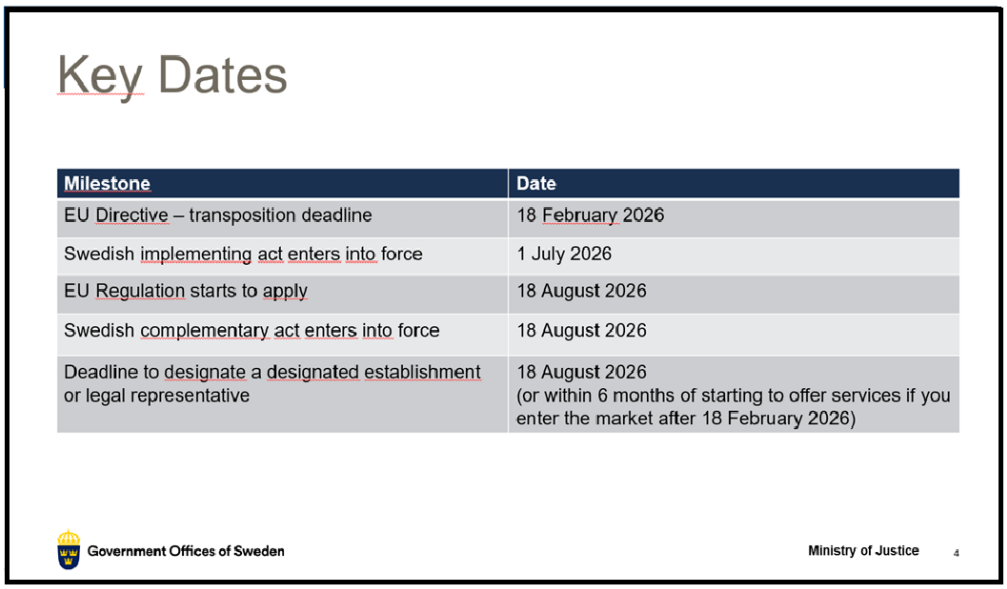
Sweden's Implementation of the E-Evidence Framework

Following the Commission's overview, **Annika Bergstedt** of the Swedish Ministry of Justice presented Sweden's national implementation.

Bergstedt described her presentation as bringing the discussion "from Brussels to Stockholm." She explained that Sweden's implementation is based on a government bill submitted to Parliament in March 2026, itself based on a government inquiry and consultation with courts, academics, industry and law enforcement.

Sweden's legislative package consists of three core elements. First, a complementary act fills in the gaps left by the directly applicable Regulation. Second, a standalone act implements the Directive on designated establishments and legal representatives. Third, amendments to existing legislation ensure oversight of European Production Orders for traffic and content data.

Bergstedt was transparent that Sweden had missed the Directive's formal transposition deadline of 18 February 2026. However, the Swedish implementing act is expected to enter into force on 1 July 2026, at which point PTS — the Swedish Post and Telecom Authority — will formally become Sweden's central authority under the Directive. The Regulation itself becomes applicable on 18 August 2026.



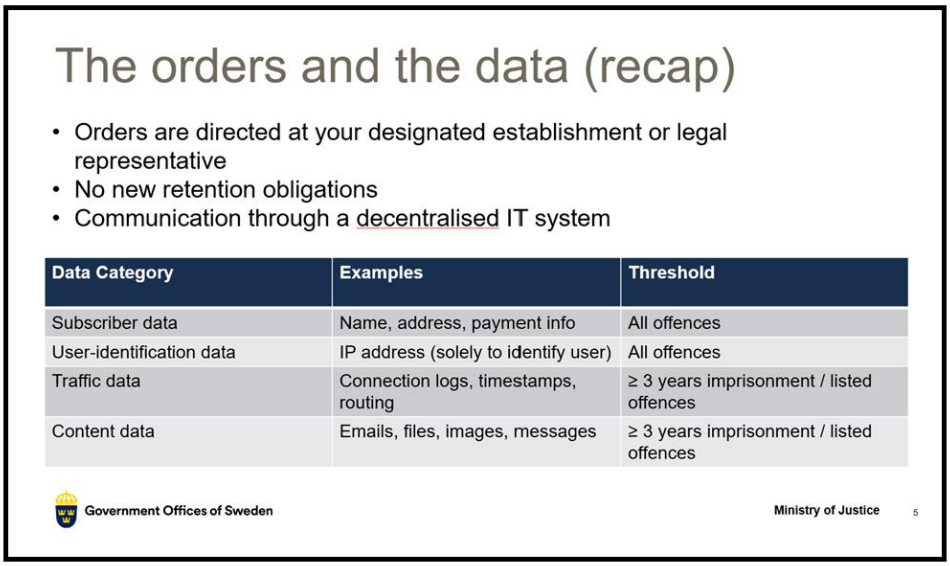
One of **Bergstedt's** key messages was that designation is "not a box-ticking exercise." A designated establishment or legal representative must have real authority, resources and operational capability. It must be able to receive orders, understand what is being requested, access relevant systems or escalation channels, preserve data, produce data and communicate with authorities within the required timelines.

She explained that providers established in Sweden and offering services cross-border are covered. Providers not established in Sweden but offering services in Sweden may also be covered, especially if they are not established in any EU Member State or are only established in a Member State that does not participate in all relevant instruments.

The Nordic context is notable. Denmark does not participate in the E-Evidence Regulation or the European Investigation Order. A provider established only in Denmark but offering services in Sweden may therefore fall under Swedish rules. A provider established in Finland, by contrast, would generally be covered by Finnish implementation.

Service providers must notify the relevant central authority of their designated establishment or legal representative. In Sweden, this means notifying PTS. Providers must supply contact details, territorial scope and accepted communication languages. Sweden will accept Swedish and English.

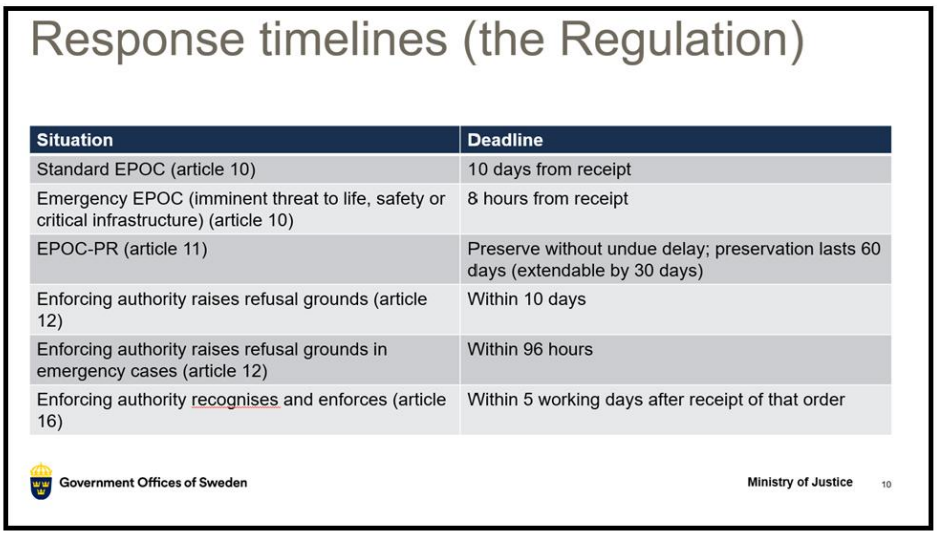
Bergstedt also explained Sweden's competent authorities. When Sweden is the issuing state, prosecutors will be competent to issue production orders for all categories of data. For traffic and content data, court approval is required. Law-enforcement agencies may issue production orders only for subscriber and user-identification data, and such orders must be approved by a prosecutor.



When Sweden is the issuing state, Swedish public prosecutors act as enforcing authorities. They may review orders, raise refusal grounds and compel compliance. The Swedish Prosecution Authority may also impose sanctions for breaches of the Regulation.

The Swedish sanctions framework is strict. PTS may impose administrative fines from 10,000 Swedish kronor up to 2% of the provider's total global annual turnover for breaches of the Directive. The Swedish Prosecution Authority may impose equivalent fines for breaches of the Regulation. Bergstedt stressed that this is a strict liability regime: the authority does not need to prove intent or negligence. The mere fact of a breach is sufficient. Joint and several liability applies between the service provider and its designated establishment or legal representative.

Bergstedt also highlighted the practical challenge of response timelines. Standard production orders generally require response within ten days. Emergency cases require action within eight hours. Preservation orders require data to be preserved without undue delay. These deadlines mean that providers must have procedures in place before requests arrive.

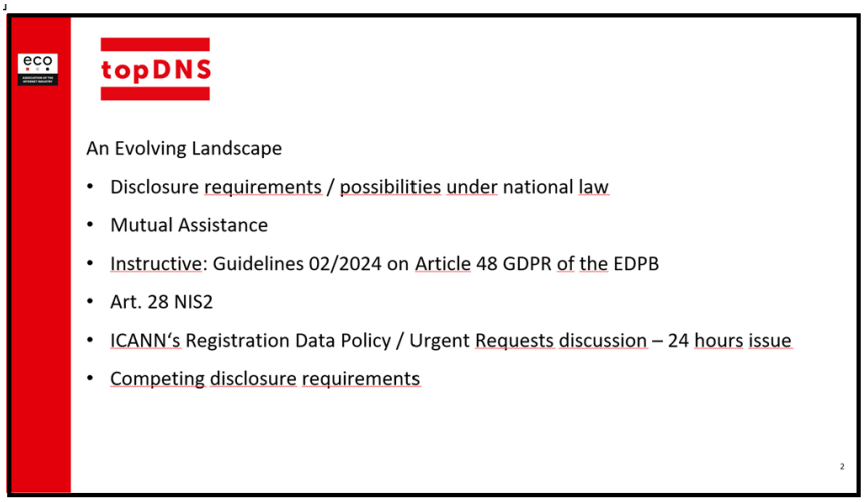


Her core message was practical: providers should designate, notify and empower their responsible entities now. While the system may start gradually, delay in preparation creates operational and legal risk.

DNS Abuse and E-Evidence: Where They Intersect

Thomas Rickert then connected the E-Evidence framework to the realities of DNS abuse mitigation and the broader regulatory environment facing Internet infrastructure providers.

Rickert's contribution was important because it moved the discussion beyond the text of the Regulation. In his view, E-Evidence should be understood as part of a wider landscape of disclosure obligations and regulatory pressure. Providers already face requirements and expectations under national law, GDPR, mutual legal assistance, NIS 2, ICANN's Registration Data Policy, urgent disclosure debates, rights-holder requests and law-enforcement cooperation. E-Evidence adds another layer to this landscape.



From a provider perspective, the challenge is increasingly not compliance with a single regulation but managing the cumulative effect of multiple overlapping regimes. Registries, registrars and hosting providers may receive requests under different legal bases, subject to different timelines, safeguards and reporting obligations. This requires organizations to establish clear internal procedures and governance structures rather than treating requests as exceptional events.

Rickert also emphasized that compliance is becoming increasingly evidence based. Providers are expected not only to maintain accurate customer data but also to demonstrate that their technical and organizational measures, escalation procedures, supplier relationships and compliance processes function in practice.

Rickert described this development as part of a broader “privatisation” of law-enforcement requests. Historically, foreign law-enforcement authorities seeking data needed to go through their own national authorities, who would then contact authorities in the provider’s country. Under E-Evidence, authorities may address certain requests directly to private service providers through their designated establishments or legal representatives.

This changes the role of providers. Registries, registrars and hosting companies are not merely passive holders of data. They increasingly become operational participants in investigations, required to preserve data, produce data, assess requests, document decisions and manage escalation.

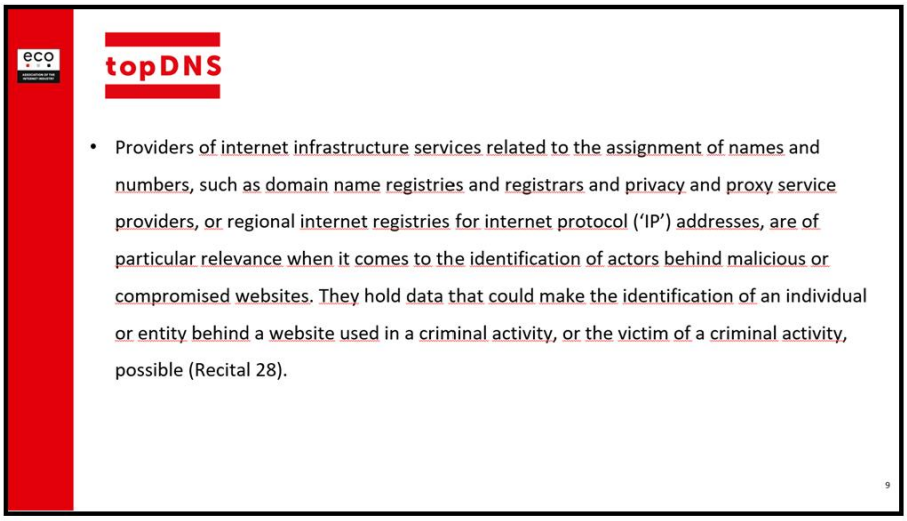
Rickert explained the different actors involved: the service provider, the designated establishment or legal representative, the issuing authority, the validating judicial authority where required, the enforcing authority, the central authority, the issuing state and the enforcing state. Understanding these roles is necessary because providers need to know who issued the request, who validated it, who may enforce it, and who may raise objections.

He also highlighted that E-Evidence relies on standardised forms. These include forms for production orders, preservation orders, non-execution, confirmation and extension. Standardisation may help structure the process, but it also means providers must be able to understand the forms and act quickly.

Rickert then explained the different data categories covered by the framework. Subscriber data may include name, address, date of birth, email address, telephone number, billing information and account details. User-identification data may include IP addresses, relevant ports and timestamps. Traffic data includes metadata such as routing, location, timing, duration, size and format. Content data includes the substance of communications, such as text, images, audio, video and files.

These distinctions are critical because different legal thresholds apply. Subscriber and identification data may be requested for a broader range of offences. Traffic and content data are subject to stricter safeguards and generally require higher offence thresholds or specific categories of serious crime.

Rickert noted that DNS abuse cases frequently intersect with the types of crime covered by E-Evidence. Phishing, malware, botnets, payment fraud, cybercrime, terrorism-related activity and child sexual abuse material may all involve domain names, hosting infrastructure or registration data.



However, he also stressed that even subscriber data can be sensitive. Identifying the registrant behind a domain name may expose journalists, activists, whistleblowers or vulnerable users. Providers must therefore take procedural safeguards seriously.

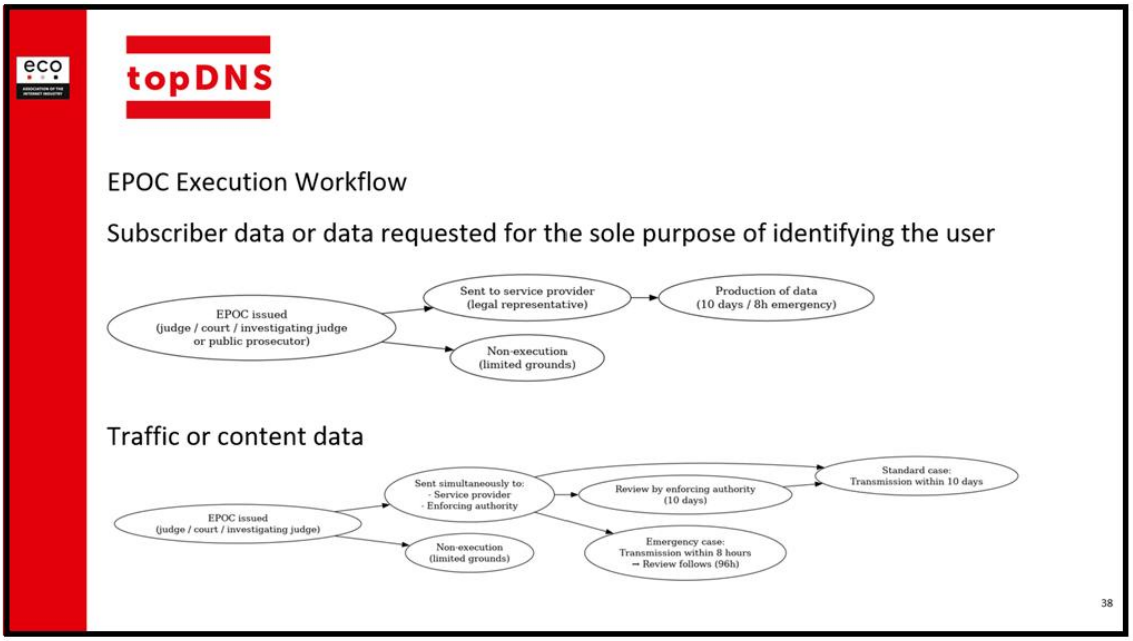
The core message of **Rickert's** presentation was that E-Evidence turns abstract regulatory compliance into a concrete operational issue. Providers must know what data they hold, how to preserve it, how to produce it, and when they may lawfully object.

Production Orders, Preservation Orders and Provider Responsibilities

A significant portion of the workshop examined what providers must actually do when an E-Evidence request arrives.

European Production Orders require providers to produce specified data. European Preservation Orders require providers to preserve data for a defined period while a later production request may be prepared. The distinction matters because the obligations, timelines and procedural consequences differ.

Thomas Rickert explained that providers must quickly answer several questions. Is the request a production order or a preservation order? Is it urgent? What category of data is being requested — subscriber data, identification data, traffic data or content data? Was the request issued or validated by the correct authority? Does the provider hold the relevant data? Is the request formally complete? Are any privileges or immunities engaged? Is there a conflict with third-country law? What deadline applies?



For many providers, these questions will require coordination between legal, technical, security and compliance teams. The legal team may assess validity and refusal grounds. Technical staff may locate and extract data. Compliance teams may document actions. Management may need to be involved in high-risk cases.

Preservation orders deserve particular attention because they are easy to underestimate. Providers may focus on production, but preservation creates its own obligations. Data must be preserved without undue delay from receipt of the order. The standard preservation period is 60 days, with a possible 30-day extension. If a subsequent production request is confirmed, preservation must continue. This requires technical capability to identify the relevant data, prevent deletion or alteration, maintain confidentiality and document what was preserved and when.

The grounds for non-execution are deliberately limited. They cover formal errors, incomplete requests, de facto impossibility, absence of the relevant data, incorrect issuing authority, privileges or immunities, or conflicts with third-country law. Providers cannot refuse because a request is inconvenient, burdensome or commercially sensitive. Understanding what the grounds actually cover — and what they do not — is essential before requests arrive.

The Eight-Hour Challenge

Among the most discussed issues in the workshop was the emergency response deadline.

In standard cases, providers generally have ten days to respond to European Production Orders. In emergency cases — defined in Article 3(18) of the Regulation as situations involving an imminent

threat to life, physical integrity or safety of a person, or serious threats to critical infrastructure — providers may have only eight hours.

The eight-hour deadline is not merely a legal detail. It is an organizational stress test.

The workshop did not suggest that providers will immediately be flooded with emergency orders. Several speakers noted that implementation may be gradual. But the legal requirement exists from 18 August. Providers that wait until the first emergency order arrives before building response capability will already be in breach.

The eight-hour challenge therefore became one of the clearest operational takeaways from the workshop: E-Evidence readiness requires more than knowledge of the law. It requires functioning internal processes.

JUDEX and Technical Readiness

After the legal and operational discussions, **Ulrich Plate** addressed the technical implementation of the framework.

Plate focused on JUDEX — the Justice Digital Exchange System — intended to support secure communication between authorities and service providers. JUDEX relies on national access points, a central database and provider-facing interfaces. Providers may connect through a web-based interface or, for higher-volume operators, an API.

Plate's presentation was a reality check. The legal framework may be set, but technical and administrative readiness remains significantly uneven. At least five Member States have confirmed they will not meet the August deadline. Most others do not yet have a designated central authority. The central database — which must contain validated provider registrations before authorities can locate and address providers — is sparsely populated. At the time of the workshop, fewer than fifty entities had completed the notification process across the entire EU. Seven organizations were actively testing the API.

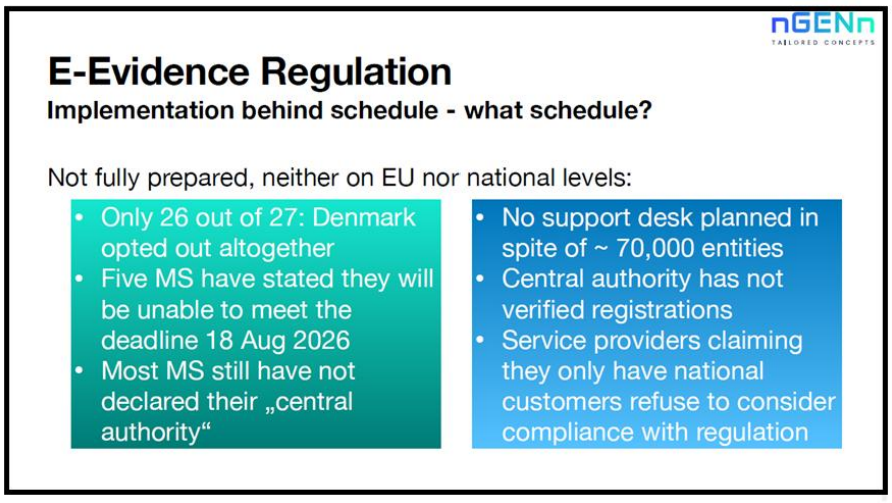


Plate walked through the notification portal live, demonstrating the registration process providers must complete. The demonstration revealed real usability concerns: mandatory fields that do not accommodate all provider types, a session timeout requiring users to restart the process if inactive for longer than five minutes, free-text service description fields conflicting with the formalized service tags used in the actual order transmission and handling, and validation dependencies on central authorities that have not yet been formally appointed in many Member States.

The fallback question is particularly unresolved. The Regulation provides for situations where the standard IT system is unavailable, requiring alternative means of communication. At present, there is no unified EU position on what those alternatives should be. Options under discussion include encrypted email and qualified electronic registered delivery services, but practical questions remain unanswered: how does an authority identify whom to contact if a provider is not yet in the central database, and how are cryptographic keys exchanged in advance?

Interaction with the Digital Services Act

Participants also raised questions about the interaction between E-Evidence requests and Digital Services Act transparency-reporting obligations. One concern was that current E-Evidence forms do not necessarily provide sufficient categorisation information to allow providers to classify requests according to the DSA's reporting framework.

Commission representatives acknowledged the issue and noted that its practical implications may need to be examined further as implementation progresses. The exchange highlighted how E-Evidence will operate alongside, rather than replace, other regulatory obligations.

Plate's framing was measured but direct. The system is not failing — significant work has been done and it is demonstrably operational in test conditions. But it will take time to mature into a system capable of handling the volumes eventually expected. Providers should prepare for both structured digital workflows and a period of transitional uncertainty. "Gradual maturation" is the honest description of what is coming.

One exchange from the floor illustrated the practical implications of **Plate's** assessment. A participant observed that the implementation challenge is not simply technical but also one of scale. In Germany alone, roughly 70,000 entities could potentially fall within the scope of the E-Evidence framework. Yet many providers remain unaware that they may have obligations under the Regulation and Directive, while the authorities responsible for validating registrations and maintaining the system currently operate with comparatively limited resources.

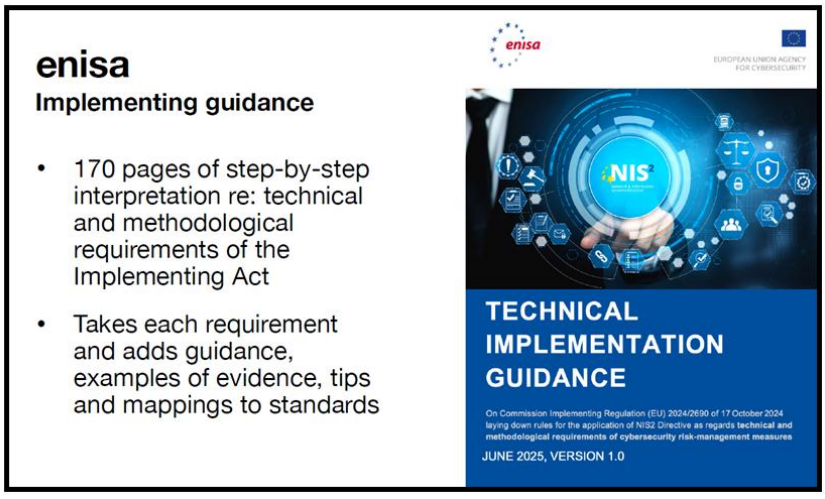
The observation highlighted a broader concern running through **Plate's** presentation. The success of the framework depends not only on the availability of systems such as JUDEX, but also on the ability of authorities and providers to complete a large-scale onboarding process within a relatively short period of time. Before authorities can issue orders efficiently, providers must first understand that they are in scope. They must then designate a legal representative or establishment where required, complete the notification process and establish the necessary operational procedures.

Several participants noted that providers that fail to engage with the process will not simply remain outside the system. They may instead become future enforcement cases. The exchange illustrated one of the workshop's recurring themes: the legal framework may now be largely complete, but the operational ecosystem required to support it is still being built. The challenge is no longer drafting the rules but making them work at scale.

E-Evidence and the Broader Regulatory Landscape

The final segment of the workshop placed E-Evidence within the wider compliance environment for digital service providers.

Ulrich Plate used NIS 2 as a key example. He explained that providers are already dealing with cybersecurity risk-management obligations, incident reporting requirements, national transposition differences and detailed "enisa" guidance. The NIS 2 implementing regulation for digital service providers expands the directive's ten risk-management principles into twenty-seven pages of specific requirements covering network security, access controls, cryptography, incident management, supply-chain security and more. "enisa" has published further guidance elaborating on implementation and cross-referencing these requirements against international standards including ISO 27001 and NIST. The significant incident thresholds specified for DNS services were noted to be considerably more demanding than what DNS operators typically regard as serious failures in practice.



What connects NIS 2, E-Evidence and the broader regulatory landscape is the shift towards evidence-based compliance. Providers must increasingly be able to demonstrate that their policies, controls and processes actually function. This means maintaining documentation — network diagrams, access-control records, audit logs, escalation procedures, incident timelines, supplier assessments — not as bureaucratic archives but as operational records that can be produced when authorities or auditors ask.

Thomas Rickert reinforced this point in his closing remarks. He argued that the cumulative weight of GDPR, ICANN's Registration Data Policy, NIS 2, E-Evidence, the DSA, national disclosure laws and supply-chain obligations is transforming what it means to operate in the domain name and hosting industry. Providers must maintain accurate customer data, documented internal processes, technical and organizational measures, contingency plans and demonstrable control over suppliers and resellers.

Rickert also argued that the cumulative weight of GDPR, ICANN's Registration Data Policy, NIS 2, E-Evidence, the DSA, national disclosure laws and supply-chain obligations is transforming what it means to operate in the domain name and hosting industry. Providers must maintain accurate customer data, documented internal processes, technical and organizational measures, contingency plans and demonstrable control over suppliers and resellers.

Key Takeaways

The 2026 E-Evidence Workshop produced several clear takeaways for the domain name and hosting industry.

- **E-Evidence becomes applicable on 18 August 2026.** The deadline is fixed regardless of how many Member States are behind schedule. Providers should not interpret slow implementation as permission to delay their own preparation.
- **DNS and hosting providers are directly in scope.** Domain name registries, registrars, hosting providers and related infrastructure operators are expressly referenced in the framework and must assess whether they are covered.
- **Designation must be genuine, not nominal.** A legal representative or designated establishment must have real authority, access, resources and operational capability. Appointments that exist only on paper will not satisfy the framework's requirements and may expose providers to sanctions.
- **Response timelines are demanding.** Standard production orders generally require response within ten days. Emergency orders may require action within eight hours. These deadlines apply from the moment the order is received.
- **Preservation obligations matter independently.** Providers must be able to preserve relevant data without undue delay. This requires technical capability before requests arrive.
- **Grounds for refusal are limited.** Providers must understand the narrow circumstances in which they may lawfully decline or delay. This requires legal preparation, not improvisation.
- **The technical system is developing but not yet complete.** JUDEX is operational in limited testing environments, but significant implementation and onboarding challenges remain. Providers should prepare for both structured digital workflows and a transitional period of mixed communication channels.
- **E-Evidence coexists with other frameworks.** NIS 2, GDPR, DSA reporting, ICANN policies and national disclosure laws remain independently applicable. Internal processes must handle requests arriving under multiple legal bases simultaneously.

- **Compliance is now evidence-based.** Providers must be able to show that processes and controls work in practice, not merely that policies exist on paper.
- **Market consolidation is a realistic consequence.** Several speakers suggested that the cumulative compliance burden may prove particularly challenging for smaller providers and could contribute to market consolidation.

Conclusion

By Nordic Domain Days 2027, E-Evidence will no longer be a forthcoming development on the compliance horizon. It will be part of the daily operating environment for European digital infrastructure providers.

The framework introduces a genuinely new model: direct orders from foreign authorities to private providers, with demanding timelines, strict liability, significant sanctions and limited grounds for refusal. For an industry already navigating DNS abuse, NIS 2, GDPR and ICANN policy evolution, it adds a substantial new operational dimension.

The workshop's overall message was not alarmist but was unambiguous. As several speakers emphasized in different ways, preparation should occur before "the first order arrives," not after. Providers that treat E-Evidence as someone else's problem — whether because they consider themselves small, domestic, peripheral or not-quite-in-scope — are taking a serious risk. The framework is broad, the sanctions are real, and the practical challenges of compliance are better addressed before the first order arrives than after.

The industry's challenge is to ensure that when abuse meets evidence, providers can respond lawfully, proportionately and effectively — and that they have built the internal capability to do so before they need it.

This report is based on the proceedings of the E-Evidence Workshop held at Nordic Domain Days 2026 in Stockholm on 26 May 2026, organized by eco's topDNS Initiative and iQ Global.