OCTOBER 2025 • *Brussels, Belgium*

CENTR Board statement on Digital Package (Digital Omnibus)

Summary of CENTR key points

- There is no added value in duplicating audits, supervisory powers and minimum cybersecurity risk-management measures across EU legislation affecting essential digital infrastructure. Further simplification and clarification are warranted, including a clear exemption for ccTLD registries from the DORA oversight framework.
- The number of audits one operator must undergo to demonstrate conformity for the same legislative requirements should be reduced to one, preferably under the main cybersecurity legislation (i.e., the NIS 2 Directive).
- The European Commission, together with EU Member States, should encourage, and where appropriate facilitate, the development of a single, secure reporting interface at the national level, tailored for each Member State.
- The European Commission should assess the overlap between different legislative instruments and exempt essential entities from reporting the same incident under multiple legislative frameworks.

Introduction

CENTR is the association of European country code top-level domain registries (ccTLDs). All EU Member States and EEA country ccTLDs (such as .de for Germany and .no for Norway) are members of CENTR.

CENTR members are at the core of the public internet, safeguarding its stability and security. The majority of European ccTLDs are non-profit organisations or SMEs, providing an internet infrastructure service in the interest of and in close cooperation with their local internet communities (e.g., end-users, CSIRTs, law enforcement and other competent authorities).

Domain names are the foundational pieces of internet infrastructure necessary for many online services (e.g., website, application, platform) to be accessible online. ccTLDs are responsible for operating and maintaining the technical Domain Name System (DNS) infrastructure for their top-level domain.

The DNS is a well-established network protocol at the heart of the internet infrastructure. It provides a navigation function to map user-friendly domain names to numeric IP addresses. ccTLD registries maintain a domain name registration database that contains technical and administrative data necessary to provide DNS services, as well as identity and contact information of domain name holders. ccTLDs are considered "essential entities" under the NIS 2 Directive[1].

In the context of the ongoing call for evidence on the Digital Package, CENTR members wish to highlight opportunities to further simplify and align reporting and cybersecurity oversight framework under different EU rules.

Audits and supervision framework

The NIS 2 Directive is the primary cybersecurity legislation relevant to maintaining the security and stability of ccTLD's technical operations. The NIS 2 Implementing Regulation[2] specifies a list of mandatory minimum risk-management measures applicable to TLD registries, as essential entities under the NIS 2 Directive.

As part of the ex-ante supervisory regime applicable to the essential entities, the NIS 2 Directive requires regular and targeted audits by supervisory authorities or independent auditors. Essential entities may also be subject to ad hoc audits following a significant incident, as well as undergo security scans in cooperation with supervisory authorities.

When it comes to the cybersecurity audit and oversight framework applicable to digital infrastructure, several pieces of EU regulation prescribe different rules that are not always aligned. As a result, an essential entity, such as a ccTLD, may be subject to overlapping rules and supervisory frameworks that attempt to establish compliance with the same or similar obligations.

DORA

DORA[3] is an EU regulation designed to strengthen the digital resilience of financial entities. It introduces certain contractual obligations for third-party ICT service providers and an extensive oversight framework for those deemed to offer 'critical' or 'important' services to financial entities. As the domain name and its underlying infrastructure are essential for providing any online service (e.g., application, platform, or website), ccTLDs fall under the scope of DORA as a third-party ICT service provider, even if a service operating on top of the domain name is provided by a different service provider (e.g., cloud or hosting provider).

Whether domain registries can be designated as 'critical' or 'important' third-party ICT service providers depends on an assessment by the European Supervisory Authorities (ESAs) that are competent under DORA. If deemed critical or important, ccTLD registries may be subject to extensive oversight by financial entities, including audits and interventions in decisions regarding their subcontractors.

The primary goal and responsibility of a ccTLD registry is to ensure the global availability, resilience and stability

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union ('NIS 2 Directive').
[2] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 ('NIS 2 Implementing Regulation')
[3] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector ('DORA').

of the DNS. The DNS supply chain is highly globalised and interconnected, since DNS availability is a key consideration in the design of the DNS ecosystem.

Although DORA is considered a *lex specialis* in relation to the NIS 2 Directive and regarding financial entities, it failed to foresee any unintended consequences for the internet's core infrastructure, such as ccTLDs, that are in a unique position within the internet's global ecosystem. The DORA oversight framework is not fit for the purpose of ensuring security, stability, and resilience of the DNS, which is governed by global international standards. Furthermore, it is unclear why financial entities are granted an extensive oversight of critical/important ICT providers, when their core business is not ICT, nor cybersecurity.

Therefore, it would be beneficial to clarify and align the two cybersecurity frameworks under DORA and the NIS 2 Directive, particularly regarding their applicability to digital infrastructure actors that are deemed essential entities under the NIS 2 Directive. There is no added value in duplicating audits, supervisory powers, and minimum cybersecurity risk-management measures in contractual obligations with financial entities, since ccTLD registries are already subject to a strict ex-ante and ex-post supervisory regime under the NIS 2 Directive. Further simplification and clarification are warranted, with a clear exemption for ccTLD registries from the DORA oversight framework.

EU Digital Identity Framework

The EU Digital Identity Framework[4] ('EUID') establishes certification and conformity rules for qualified trust service providers, who are subject to regular audits every 24 months by a conformity assessment body. These audits shall confirm that the qualified trust service providers fulfil the minimum cybersecurity risk management measures stipulated in the NIS 2 Directive.

Trust service providers are similarly covered by the NIS 2 Directive as essential entities that are subject to an ex-ante and ex-post regime, as part of the digital infrastructure block. Like other digital infrastructure providers, trust service providers are also subject to regular audits and security scans under the NIS 2 Directive regime. While the EUID framework provides for additional assurance levels for trust service providers to achieve the "qualified" status, it is unclear why qualified trust service providers should be subject to additional conformity checks for the same requirements they are already covered by, without being considered "qualified". This simply creates an additional level of complexity and bureaucracy for operators, without increasing security.

Additionally, it is worth mentioning that an operator can simultaneously be considered a trust service provider, a qualified trust service provider, and a DNS service provider, and subject to three different audits for essentially the same legislative requirements. It seems that the legislative frameworks of both the EUID and the NIS 2 Directive were designed without considering this potential overlap. This can essentially create a significant burden for operators to consider additional business opportunities.

At a minimum, the number of potential audits that an operator must undergo to demonstrate conformity with the same legislative requirements should be reduced to one, preferably under the main cybersecurity legislation (i.e., the NIS 2 Directive). To simplify the existing rulebooks and promote the uptake of new business opportunities across sectors, the audit and oversight framework should be service-based, rather than operator-

[4] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework ('EUID').

wide. Where services overlap or are covered by existing EU or national audits, operators should also be able to demonstrate conformity with additional requirements by recognising existing audit results as valid.

The CER Directive[5] sets a positive precedent by recognising that the NIS 2 Directive already imposes extensive cybersecurity requirements on a wide range of entities. As cybersecurity is sufficiently addressed in the NIS 2 Directive, digital infrastructure entities, including ccTLDs, are exempt from the CER Directive's incident reporting and audit provisions. The European Commission should adopt a similar approach in any EU legislation containing cybersecurity elements.

Cybersecurity-related incident reporting obligations

ccTLDs are subject to reporting obligations for cybersecurity incidents and data breaches, primarily under the NIS 2 Directive and the GDPR[6].

Although these pieces of legislation cover different areas, there may be instances of reporting overlap when incidents within the technical operation of a TLD also involve personal data breaches. Double reporting obligation in this case could place an additional burden on the operator and create informational silos for the competent authorities.

Consequently, there is an opportunity to streamline reporting mechanisms to enable a more timely and efficient response to cybersecurity incidents involving personal data breaches.

Single reporting mechanism

Submitting reports under different legislation can be unnecessarily complex, as affected entities may be required to navigate diverging reporting templates across different platforms. Manually entering similar information on different platforms and reporting mechanisms increases the risk of human error and inconsistencies in submitted reports to different competent authorities. In some Member States, there is no interface to report an incident or a data breach. Instead, email communication with the authorities is relied upon.

A single secure interface[7] at the national level would simplify the reporting, as information would only need to be submitted once. Furthermore, affected entities would only need to work on one comprehensive reporting narrative containing all the necessary information, rather than tailoring their reports to the relevant authority.

The European Commission should work together with the Member States to facilitate the development of a single and secure reporting interface at the national level, tailored for each Member State.

Reporting timelines

Incident reporting obligations under different EU legislation relevant to cybersecurity follow different reporting timelines. Under the NIS 2 Directive, the timeline includes an early warning to CSIRT or a competent authority within 24 hours of becoming aware of the significant incident, an incident notification within 72 hours of becoming aware of the significant incident, and a final report no later than one month after the submission of

[5] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities ('CER Directive').
[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ('GDPR').
[7] Existing cybersecurity incident reporting platforms found across Member States could be potentially explored to allow broader incident reporting to different authorities. For example, Lucia in Spain, IRON in Sweden, or Safeonweb in Belgium.

the incident notification.[8] Under the GDPR, the notification of a personal data breach must be reported to the relevant data protection authority without undue delay and no later than 72 hours after becoming aware of it.

A significant incident[9] under the NIS 2 Directive may trigger the need to file a data breach notification under the GDPR. Under the AI Act[10], the obligation to report incidents involving AI systems used in digital infrastructure, such as ccTLD registries, should only apply to the violation of fundamental rights. While the European Commission's draft guidance on serious AI incidents includes a list of examples of such infringements[11], it is unclear how this obligation interacts with the reporting obligations under the GDPR. The timeline for reporting significant incidents under the AI Act for deployers of high-risk AI systems across essential digital infrastructure is no later than within 24 hours.

In practice, the overlapping timelines and reporting obligations mean that affected entities would have to manage several reporting streams under different timelines in parallel, while essentially reporting the same incident. Aligning reporting timelines could therefore reduce the reporting burden for non-profit organisations and SMEs, while contributing to increased legal clarity for providers of essential digital infrastructure. If the same incident falls under the reporting obligations of different EU legislation across sectors, it would be beneficial to submit it once through a single reporting mechanism within the same timeline, and with the automatic involvement of several competent authorities. This would prevent operators from risking non-compliance by missing a deadline. Additionally, one incident report covering multiple areas must remain within the reasonable timeline that does not shorten any existing deadlines currently applicable to operators. Most importantly, the incident should be reported, for the affected entity and the competent authority to address and mitigate the aftermath of the incident.

Consequently, the European Commission is encouraged to assess the potential overlap between different legislative instruments, exempting essential entities from the obligation to report the same incidents under multiple legislative frameworks and different timelines.

Furthermore, EU policymakers are strongly encouraged to avoid introducing additional complexity to incident reporting procedures and timelines when introducing new EU legislation affecting essential digital infrastructure. Therefore, it is imperative that, when revising or adopting EU legislation, the reporting procedures and timelines are aligned as much as possible.

[8] A similar three-step reporting approach is also found in the Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements ('Cyber Resilience Act').
[9] For TLD registries, Article 6 of the NIS 2 Implementing Regulation.
[10] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence ('AI Act')
[11] The European Commission, Draft Guidance Article 73 AI Act - Incident Reporting (High-Risk AI Systems), 26 September 2025.