E-Paper

NIS2

Unraveling the Directive

Insights for operators & domain experts.



TABLE OF CONTENTS

Executive Summary 03

Introduction 04

Chapter 01: NIS2 Directive: A new chapter in EU cybersecurity 05

Bolstering the EU's cybersecurity strategy
Bridging the cyber gap: NIS2 Directive's role in the EU ecosystem
The three pillars of NIS2 to enhance cybersecurity
From NIS1 to NIS2: A breakdown of the critical changes

Chapter 02: Who must comply with the NIS2 Directive? 10

Understanding essential and important entities in the NIS2 Directive
Digital infrastructure and ICT entities in the NIS2 Directive
Regulatory requirements of the NIS2 Directive
Non-compliance consequences under NIS2

Chapter 03: NIS2 for digital infrastructure operators and domain experts 15

Navigating the ambiguity of the NIS2 Directive in the domain industry
The challenges of the NIS2 Directive for the domain industry
Meeting NIS2 Directive challenges for digital infrastructure operators
Conclusion.
InterNetX is your ally in tackling NIS2 challenges and beyond

About 24

03



Executive Summary



The shift towards digitalization, heightened by the COVID-19 crisis, has broadened the scope of threats and introduced new challenges that demand more robust, tailored solutions. Cyber risk has prompted national and European lawmakers to bolster defenses against cyber attacks. As part of this effort, the European Parliament has recently approved the Network and Information Security (NIS2) Directive, which aims to enhance security systems across an expanding range of sectors to prevent and combat cyber threats. The NIS2 Directive, an evolution of NIS1, mandates that companies within its scope implement appropriate and proportionate technical and organizational measures to manage cyber risks effectively. Furthermore, companies that fall under its power must take preventative actions and minimize the impact of any security incidents—a legislative burden to unravel for all medium and large companies.

This e-paper contains a comprehensive guide and examination of the most significant provisions put forward by the NIS2 Directive, offering valuable insights and guidance specifically tailored for digital infrastructure operators and domain experts. **However**, we would like to draw your explicit attention to the fact that this e-paper is intended for information purposes only. It does not constitute legal advice and cannot replace legal counseling in individual cases.

Who will find this e-paper valuable?
This e-paper is directed towards digital infrastructure professionals, such as network administrators, telecommunications engineers, IT managers, and domain professionals, among others. However, the information in these pages will also be valuable to decision-makers, executives and other stakeholders involved in the digital infrastructure and DNS sector as well as those who wish to better understand the NIS2 Directive and its implications for their work.

Key takeaways

- The EU cybersecurity landscape, including its regulatory framework
- The NIS2 Directive's scope, provisions and updates from the NIS1 Directive
- The main objectives of the NIS2 Directive
- Organizations and sectors required to comply with the NIS2 Directive
- The potential impact on domain experts and digital infrastructure operators
- Insights into the future outlook of EU legislation

04

EU NIS2



Introduction

In the ever-evolving cybersecurity landscape, the European Union (EU) has taken significant steps to address the increasing threats to its digital ecosystem. As the digital world advances, so must the legislation governing it. In this framework, the NIS2 Directive, building upon the foundations of the NIS1 Directive, serves as a crucial instrument in bolstering the resilience and security of the EU's critical infrastructures, fostering cross-border cooperation and promoting a culture of risk management and preparedness among organizations and stakeholders across the region.

The NIS2 Directive sets forth a range of requirements that must be adhered to, affecting aspects such as security, privacy, and interoperability. Failure to comply with these regulations can result in severe financial penalties and reputational damage, so a thorough understanding of the Directive is crucial. As digital infrastructure operators and domain experts, you are at the forefront of technological advancements and innovations. It cannot be overstated that it is imperative to understand the NIS2 Directive. Mastering its implications is critical to running a successful business, ensuring compliance with the law and contributing to a more secure and resilient digital environment across the European Union.

This e-paper provides an in-depth guide in order to enhance your understanding of the Directive, its main objectives and the compliance requirements that will impact your business. Furthermore, these pages will delve into the sectors and organizations that must adhere to the NIS2 Directive, detailing how the legislation affects domain experts and digital infrastructure operators. Finally, we'll explore the future outlook of EU cybersecurity legislation and its potential influence on the ever-evolving cybersecurity landscape.

We invite you to embark on this journey with us. We will guide you through the intricacies of the Directive, offering valuable insights on how to effectively navigate the compliance process and the potential impact on your operations. Empower yourself with the knowledge and information necessary to ensure the ongoing success of your organization.

The NIS2 Directive in numbers

18 critical sectors which are subject to the regulations set forth by the NIS2 Directive.

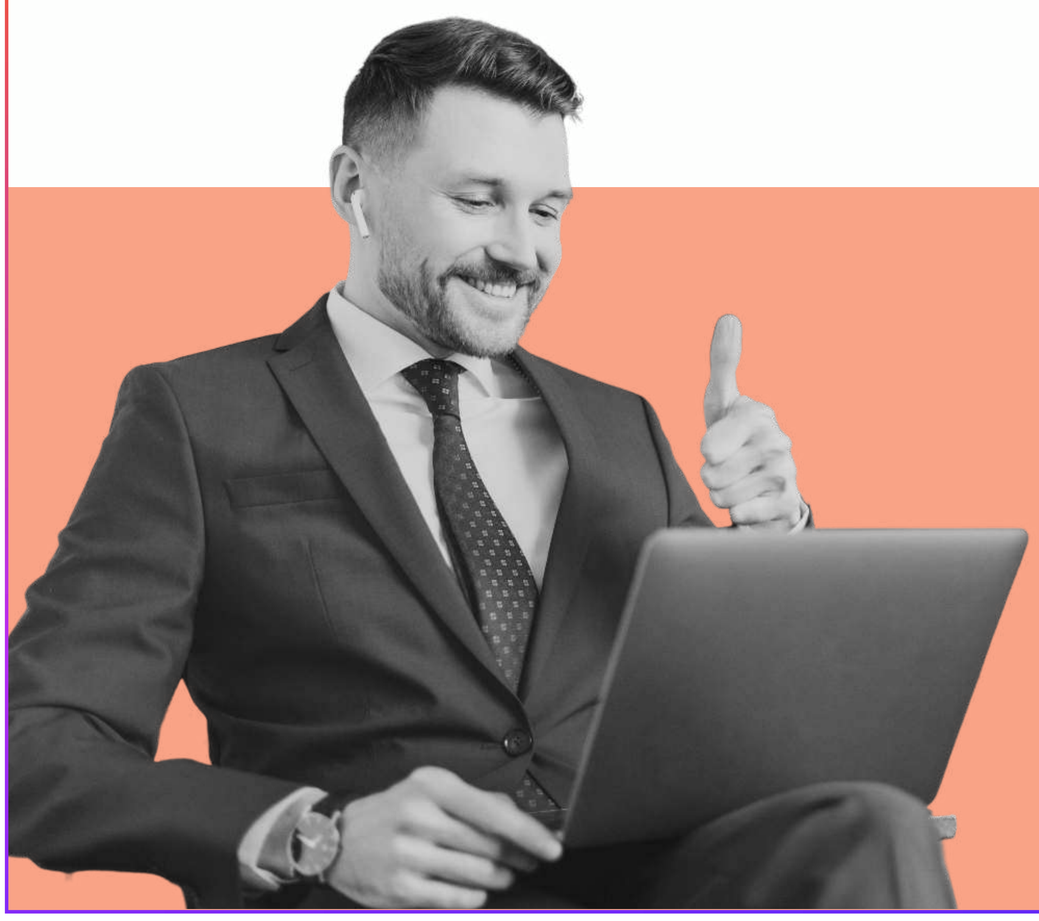
27 EU member states that are required to implement the NIS2 Directive into their national legislation.

24 hours within which organizations share an early warning indicating whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact.

46 articles in the NIS2 Directive.

72 hours within which organizations must report an initial assessment of the significant incident, including its severity and impact.

73 pages of the Directive.



CHAPTER
01

NIS2 Directive: A new chapter in EU cybersecurity

On 16 January 2023, the **NIS2 Directive (EU) 2022/2555** came into effect, superseding the previous **Directive (EU) 2016/1148**. The NIS2 Directive is a piece of EU-wide legislation on cybersecurity that aims to achieve a high common level of cybersecurity across the member states. It is designed to

- address the growing threats posed by digitalization and the surge in cyber attacks
- strengthen security requirements
- manage the security of supply chains
- streamline reporting obligations
- introduce more stringent supervisory measures and stricter enforcement requirements.

Furthermore, NIS2 expands the scope by effectively obliging more entities and sectors to take action, increasing the levelof cybersecurity in Europe in the longer term.

Full name

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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

06

Bolstering the EU’s cybersecurity strategy

As digital infrastructure operators and domain experts, comprehending the current cybersecurity landscape and its vulnerabilities is essential for grasping the implications of the NIS2 Directive. Cyberattacks are projected to increase and become more sophisticated, incorporating cutting-edge technologies and utilizing diverse exploitation methods to circumvent existing defense systems.

ENISA, the European Union Agency for Cybersecurity, reports that in 2022, the median direct cost of a substantial security breach surged to €200,000, doubling the figure from the previous year and emphasizing the escalating financial consequences of such incidents. The 2017 WannaCry ransomware attack is a prime example. It impacted over 300,000 computers across 150 countries, with damages amounting to billions. The proliferation of smart devices, cloud computing, online profiles, social media, government digital IDs and domain vulnerabilities has provided cybercriminals with a wide array of innovative avenues to exploit, leading to increasingly advanced attacks. These attackers may now use artificial intelligence and deep learning to develop new, unanticipated strategies.

Domain security is crucial in protecting digital infrastructure, as attackers often target domains to gain unauthorized access or disrupt services. Securing your domain against **DNS attacks** and **DDoS attacks** is a critical aspect of a comprehensive cybersecurity strategy.

Addressing the emerging diverse and hybrid threats is particularly challenging for digital operators, as their complex nature and individualized targeting make them difficult to detect and defend against. As a result, detection mechanisms necessitate improved correlation capabilities to connect seemingly unrelated events, including those involving domain security breaches. The NIS2 Directive acknowledges and addresses this dynamic cybersecurity environment, ensuring that Europe’s digital infrastructure, including domain security, remains robust and secure in the face of contemporary threats. Ultimately, this reduces



07

Bridging the cyber gap: NIS2 Directive's role in the EU ecosystem

As digital dependency grows, the EU continues to enhance its cybersecurity measures and adapt to new challenges. The upcoming NIS2 Directive will strengthen the EU's cybersecurity framework by addressing existing gaps and setting new standards.

The central goals of the EU's cybersecurity ecosystem are to

- ensure a high level of network and information security
- promote collaboration within and across member states
- foster innovation and research
- raise awareness among citizens and businesses about the importance of cybersecurity

Historically, the EU has prioritized cybersecurity in response to the ever-increasing threats posed by cyberattacks and digital vulnerabilities. The first major legislative initiative was the **2013 Cybersecurity Strategy**, which established the **European Union Agency for Network and Information Security (ENISA)** and paved the way for a more comprehensive approach to cybersecurity. In 2016, the EU enacted the **Network and Information Security (NIS) Directive**, its first legislation targeting cybersecurity. The EU has run various initiatives, such as creating national **Computer Security Incident Response Teams (CSIRTs)** and implementing the **EU Cybersecurity Certification Framework**.

The **Cybersecurity Act of 2019** reinforced ENISA's role and introduced a certification framework for ICT products, services and processes. The European Commission's ambitious **Digital Decade Agenda 2030** further emphasizes the need for resilient and secure digital infrastructure, including the development of joint cybersecurity capabilities.



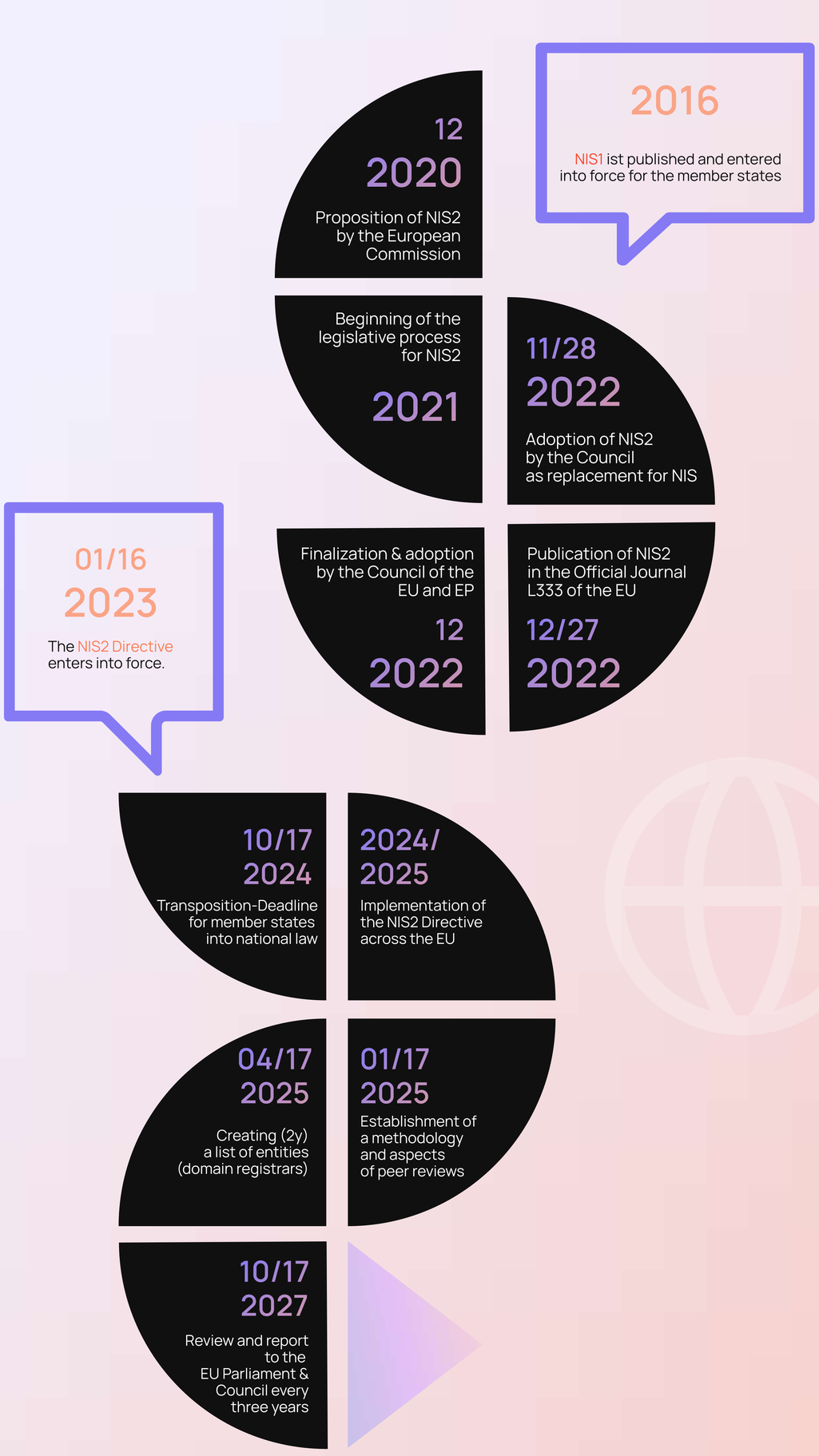
The NIS Directive laid the foundation for a harmonized and resilient cybersecurity framework across EU member states. Still, since its implementation in 2016, the risk environment has undergone significant transformations, necessitating a comprehensive update and expansion of the Directive to effectively address present and forthcoming threats, including the security of 5G technology. Amidst the pandemic, it has become increasingly evident that readying the EU for the digital era and consistently enhancing cyber-resilience is crucial, especially for operators in critical sectors. The NIS2 Directive seeks to close the gaps in the EU cybersecurity ecosystem by establishing a high common level of cybersecurity across the member states. As the digital landscape evolves, the EU must continue to invest in cybersecurity measures and adapt to new challenges.

The three pillars of NIS2 to enhance cybersecurity

The NIS2 Directive has been designed to address the deficiencies identified in the original NIS Directive, thereby strengthening the cyber resilience of businesses within the European Union. Recognizing the importance of fortifying defenses against cyber threats, the NIS2 Directive focuses on three key areas in which the original legislation fell short.

With these improvements, the NIS2 Directive aspires to create a more secure and resilient digital environment for businesses and citizens within the EU.

Roadmap of the NIS2 Directive



Enhancing cyber resilience of businesses
The NIS2 Directive acknowledges that businesses in the EU currently lack sufficient cyber resilience, which encompasses resistance to potential cyberattacks, the ability to maintain capacity during an attack as well as the capacity to recover to the original state quickly after an attack. The NIS2 Directive introduces stricter security requirements and comprehensive risk management strategies to tackle this issue and mandates regular security assessments. These measures aim to bolster the cyber resilience of businesses, ensuring they can effectively prevent, withstand and recover from cyberattacks.

Harmonizing cyber resilience across member states and sectors
Inconsistency in cyber resilience measures between member states and sectors was a significant concern under the original NIS Directive. To address this disparity, the NIS2 Directive establishes a more unified approach, extending its scope to cover additional sectors and subsectors. By implementing a harmonized set of rules across the EU, the NIS2 Directive aims to create a level playing field for businesses, fostering a more robust and consistent cyber resilience framework throughout the region.

Improving understanding and joint crisis response among member states
The NIS2 Directive recognizes that insufficient understanding of present threats and challenges and a lack of joint crisis response mechanisms have hindered the effectiveness of the original Directive. The NIS2 Directive calls for enhanced cooperation and information sharing between member states to remedy this. The EU also introduces a framework for joint crisis management, enabling a coordinated response to large-scale cyber incidents. This collaborative approach will equip member states with the necessary tools and knowledge to identify and address emerging threats, fostering a more resilient and secure digital landscape in the EU.

09

From NIS1 to NIS2.
A breakdown of the critical changes

The NIS2 Directive marks a significant milestone in the evolution of cybersecurity regulations in the European Union. While the NIS1 Directive was instrumental in setting a baseline for cybersecurity standards across various critical infrastructure sectors, the NIS2 Directive brings several enhancements and improvements that address emerging threats and vulnerabilities.

1. **Sector differentiation** – The NIS2 Directive introduces a differentiation between “essential” and “important” sectors. They must comply with the same obligations but essential entities are subject to stricter enforcement measures and sanctions.

2. **Larger scope** – The Directive expands the number of affected sectors, with critical essential entities now encompassing eleven sectors and important entities extending to seven sectors - totaling eighteen NIS2 sectors.

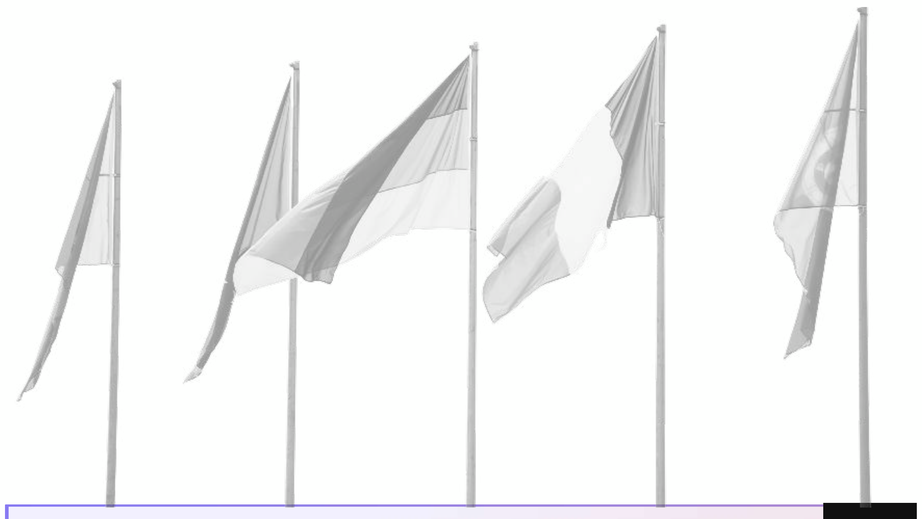
3. **Operators** – Medium and large enterprises with 50 or more employees or a turnover of at least € 10 million are impacted. There are no facility thresholds or similar limitations. Some operators, such as those in digital infrastructure and public administration, will be regulated regardless of size.

4. **Cybersecurity** – The NIS2 Directive raises cyber security requirements for operators and member states. Additionally, it emphasizes the importance of addressing cybersecurity concerns within supply chains.

5. **Cooperation** – The Directive fosters more profound supervision and collaboration between EU authorities and operators while refining European jurisdiction.

6. **Information sharing** – Another critical improvement is that member states must establish computer security incident response teams (CSIRTs) to facilitate cross-border cooperation and information sharing during cybersecurity incidents. This approach recognizes the transnational nature of cyber threats and the need for coordinated responses to mitigate their impact.

7. **Sanctions** – Penalties and enforcement actions have been significantly expanded under the NIS2 Directive. Infringements can result in fines of at least € 7 million or a maximum of € 10 million, depending on the sector.



KRITIS & NIS2 Directive: What’s the difference?

KRITIS and NIS2 Directive are two different methods for protecting critical infrastructure. KRITIS (short for Critical Information Infrastructure) is based on the German BSI Kritis Regulation and aims to identify and secure important services in sectors like energy, healthcare and transportation within Germany. The NIS2 Directive adopts a broader perspective, aiming to enhance the overall cybersecurity of critical infrastructure and digital service providers across all EU member states. While both frameworks share the common goal of safeguarding vital assets, they differ with regard to their geographical scope and the specific sectors they encompass.

GDPR & NIS2 Directive: What’s the difference?

The GDPR and NIS2 Directive are regulatory frameworks within the EU but differ in their focus. GDPR protects the privacy rights of individuals by laying down rules for the collection, processing, storage and sharing of personal data. The NIS2 Directive is centered on enhancing the security of network and information systems in various sectors and digital service providers against cybersecurity threats. Both frameworks ensure a safe and secure digital environment for businesses and consumers. GDPR applies to all EU member states directly and becomes law without further action by governments. NIS2, however, needs incorporation into the laws of each member state. The EU sets cybersecurity standards, but each state must create its own laws to implement NIS2.



CHAPTER

02

Who must comply with the NIS2 Directive?

"In order to ensure a clear overview of the entities falling within the scope of this Directive, member states should establish a list of essential and important entities as well as entities providing domain name registration services."

NIS2 Directive Recital (18)

As the EU endeavors to safeguard its digital ecosystem, understanding the obligations and requirements of the NIS2 Directive is crucial. Who must comply with this critical cybersecurity legislation? The NIS2 Directive targets a wide range of entities, including operators of essential services (OES), digital service providers (DSPs) and even certain public administration entities. These organizations span various sectors, from energy and transport to banking and health, which are vital in maintaining the stability and well-being of the EU's digital ecosystem. To mitigate cybersecurity risks and enhance digital resilience, these entities must adhere to the NIS2 Directive's stringent standards and practices.

Understanding essential and important entities in the NIS2 Directive

One of the key aspects of NIS2 is the distinction it makes between essential entities and important entities based on Article 3.

Essential entities are organizations that play a crucial role in maintaining the economy's and society's proper functioning. These organizations typically operate in the energy, transport, banking, healthcare and digital infrastructure sectors. The failure or compromise of an essential entity's network and information systems could have significant consequences, leading to large-scale disruptions, financial losses or even threats to public safety. Regardless of size, top-level domain name registries and DNS service providers are considered essential entities.

On the other hand, important entities may have a different level of criticality than essential entities. However, their smooth functioning still contributes significantly to the economy and society. Important entities include specific organizations in the digital sector, such as cloud service providers, social networks and search engines. Although disrupting an important entity's network and information systems might not result in immediate large-scale consequences, it could still substantially impact the economy or the public's trust in digital services.

Sectors with high criticality (Annex I)

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (B2B)
- Public administration
- Space

Other critical sectors (Annex II)

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food
- Manufacturing
- Digital providers
- Research



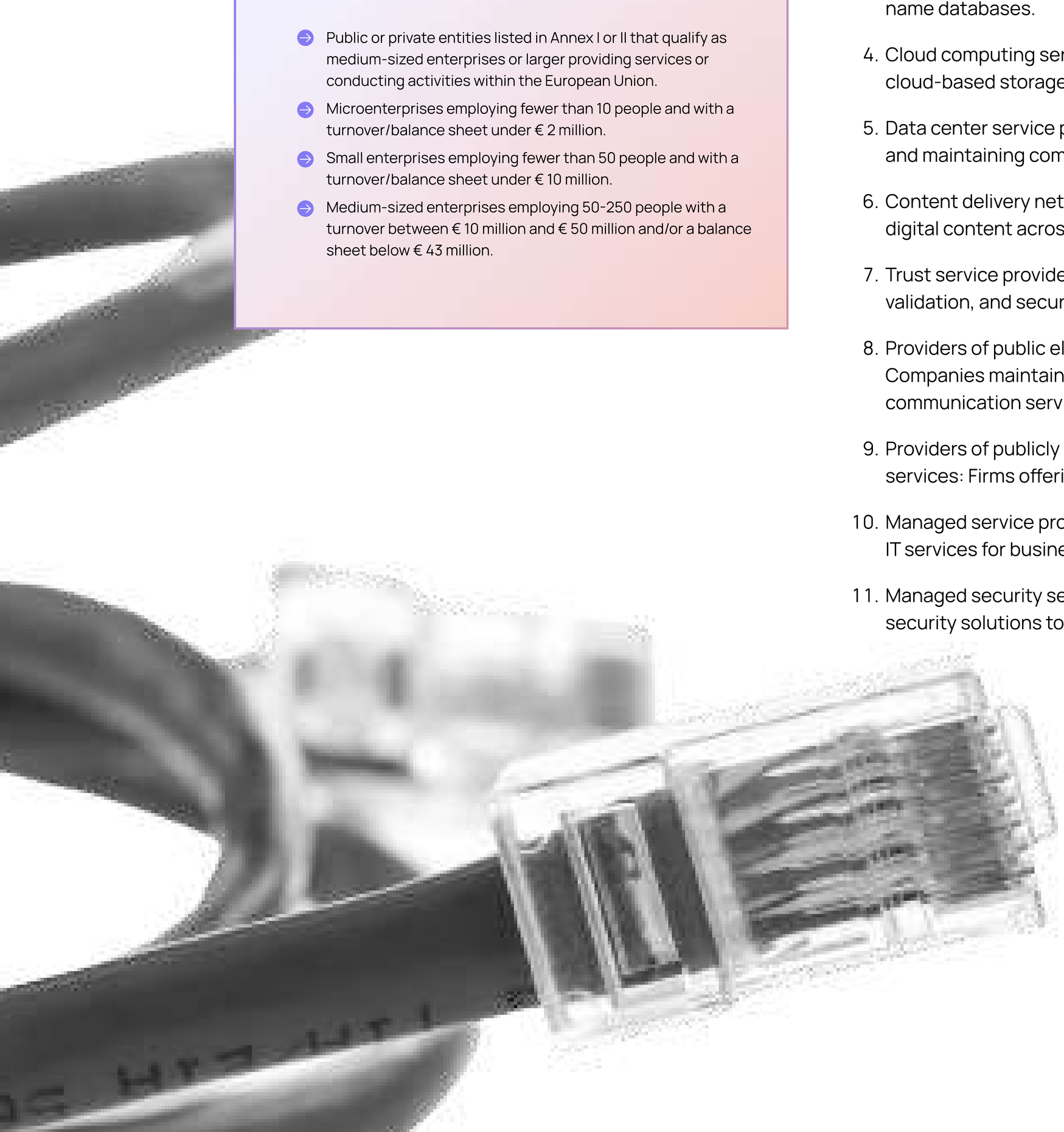
Digital infrastructure and ICT entities in the NIS2 Directive

To fully understand the scope and impact of this Directive, it is essential to identify the entities required to comply with its provisions. The NIS2 Directive lists 18 sectors that are required to comply with the Directive. Annex I and Annex II identify specific entities within the digital landscape that are required to adhere to the provisions of the NIS2 Directive.
Annex I of the Directive lists 11 sectors with high criticality, including digital infrastructure. The Annex II of the Directive lists 7 "other critical sectors".

Who must comply with the NIS2 Directive?

Under Article 2, the NIS2 Directive applies to:

- Public or private entities listed in Annex I or II that qualify as medium-sized enterprises or larger providing services or conducting activities within the European Union.
- Microenterprises employing fewer than 10 people and with a turnover/balance sheet under € 2 million.
- Small enterprises employing fewer than 50 people and with a turnover/balance sheet under € 10 million.
- Medium-sized enterprises employing 50-250 people with a turnover between € 10 million and € 50 million and/or a balance sheet below € 43 million.



Entities in the digital infrastructure and ICT sectors Annex I outlines various entities operating within the service management sectors for digital infrastructure and information and communications technology (ICT), specifically for business-to-business (B2B) applications. These entities provide the necessary services, support, and infrastructure to enable seamless and efficient digital business operations.

The list includes

1. Internet exchange point providers: Organizations facilitating Internet traffic exchange between networks.
2. DNS service providers: Companies offering domain name system services, excluding root name server operators.
3. TLD registries: Organizations managing top-level domain name databases.
4. Cloud computing service providers: Companies offering cloud-based storage, processing, and management solutions.
5. Data center service providers: Firms responsible for housing and maintaining computing infrastructure.
6. Content delivery network providers: Services distributing digital content across the internet.
7. Trust service providers: Entities offering authentication, validation, and secure communication solutions.
8. Providers of public electronic communications networks: Companies maintaining networks for electronic communication services.
9. Providers of publicly available electronic communications services: Firms offering communication services to the public.
10. Managed service providers: Companies providing outsourced IT services for businesses.
11. Managed security service providers: Firms offering specialized security solutions to protect and monitor IT systems.

Regulatory requirements of the NIS2 Directive

The Directive seeks to establish harmonized security measures and incident reporting requirements across the EU while promoting cooperation between member states in sharing intelligence on threats and exchanging best practices. Under the NIS2 Directive, companies operating in specific critical sectors must take appropriate and proportionate technical, operational and organizational measures to manage cybersecurity risks and prevent and minimize the impact of potential incidents.

Essential entities face stricter supervision, while important entities may follow a somewhat lighter approach, only documenting compliance after a significant incident or threat occurs. They will only be supervised after such incidents.

The minimum required and reviewed cybersecurity risk-management measures according to Article 21 of the NIS2 Directive:

- Risk analysis & security policies
- Significant incident handling
- Business continuity & crisis management
- Supply chain security
- Network & system acquisition, development and maintenance security
- Basis cyber hygiene practices and cybersecurity training
- Auditing/review
- Governance & personnel (human resources security, access control policies and asset management)
- Cryptography and encryption technologies
- Multi-factor authentication

Does NIS2 mandate the implementation of encryption?

NIS2 makes encryption explicitly mandatory only “for providers of public electronic communications networks or of publicly available electronic communications services” (Recital 98).

Although not explicitly mandated for other sectors, encryption technologies could be considered a necessary component of a comprehensive security strategy for digital infrastructure operators and domain experts seeking to comply with the NIS2 Directive. It emphasizes the importance of implementing appropriate and proportionate technical and organizational measures to ensure high security for network and information systems. This includes preserving the confidentiality, integrity, and availability of data.

End-to-end encryption is a widely recognized and recommended security practice and it protects sensitive information. Its adoption can help organizations meet the security requirements outlined in the NIS2 Directive.

Non-compliance consequences under NIS2

Should a business fail to comply with the NIS2, it can face significant repercussions, including substantial financial penalties, reputational damage and potential loss of essential services. Regulatory authorities can impose fines, issue injunctions and mandate corrective actions to ensure compliance. Additionally, non-compliant businesses may face increased scrutiny from customers and investors, leading to decreased revenue and reduced market share. Adhering to NIS2 is crucial for companies to maintain a secure, reliable and trustworthy digital infrastructure.

Fines

Based on Article 34, companies will be subject to fines if they do not comply with NIS2 by 2024.

- Essential companies: up to €10 million or 2% of their global annual revenue.
- Important companies: up to €7 million or 1.4% of their global annual revenue.



The NIS2 Directive in a nutshell

- is a legal measure that aims to boost the overall level of cybersecurity in the European Union.
- is expected to be formally adopted by member states in the coming months.
- implements mandatory, reviewable and sanctionable cybersecurity measures for risk management, security governance, incident reporting and recovery, resilience, as well as network, system and application security.
- calls for risk assessments of security protocols for major connected third-party service providers.
- monitors medium and large corporations in a defined list of key sectors.
- impacts heavily digital infrastructure operators, which include technology providers like data centers, content delivery networks and trust services providers.
- applies to all providers of DNS services along the DNS provisioning and resolution chain that are important for the internal market, including top-level-domain (TLD) name servers and authoritative name servers for domain names and recursive resolvers.
- can result in significant financial penalties and reputational damage for non-compliance.



CHAPTER

03

NIS2 for digital infrastructure operators and domain experts

The NIS2 Directive brings about noteworthy changes for digital infrastructure operators and domain experts. Specifically, Articles 27 and 28 tackle these crucial components by concentrating on establishing registries and maintaining domain name registration data. To meet these objectives, domain businesses must adopt updated standards, reinforce cybersecurity protocols, incorporate risk management strategies and create incident reporting systems. In the subsequent analysis, we will explore the particular effects of the NIS2 Directive on these specialists, highlighting the obstacles and prospects they encounter while navigating the ever-changing landscape of cyber threats.

> "Upholding and preserving a reliable, resilient and secure domain name system (DNS) are key factors in maintaining the integrity of the internet and are essential for its continuous and stable operation, (...). Therefore, this Directive should apply to top-level-domain (TLD) name registries, and DNS service providers (...)."
>
> NIS2 Directive, Recital (32)

Article 27: Registry of entities

> "ENISA shall create and maintain a registry of DNS service providers, TLD name registries, entities providing domain name registration services, (...). Upon request, ENISA shall allow the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable."
>
> NIS2 Directive, Article 27(1)...

Under **Article 27**, ENISA must create and maintain a registry of various entities, including DNS service providers, TLD name registries, entities providing domain name registration services, data center service providers, content delivery network providers and others. This registry aims to centralize information about these entities, ensuring proper oversight and facilitating cooperation among the competent authorities in member states.

To establish this registry, member states must require the entities mentioned in Article 27(1) to submit specific information to their competent authorities by 17 January 2025. The required information includes the entity's name, relevant sector, address, up-to-date contact details, the member states where services are provided and IP ranges. Member states must also ensure that these entities notify the competent authority of any changes to the submitted information within three months. The single point of contact for each member state will forward this information to ENISA without delay.

Article 28 – Database of domain name registrations data

> "For the purpose of contributing to the security, stability and resilience of the DNS, member States shall require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database (...)."
>
> NIS2 Directive, Article 28(1)

Article 28, in particular, is of significant importance for the domain industry. It emphasizes the need for TLD registries and domain name registration service providers to collect and maintain accurate, comprehensive data on domain name registrations. To achieve this, member states are required to ensure that their domain name registration databases include essential information such as:

- **the domain name**
- **registration date**
- **registrant's contact details**
- **domain name administrator's contact information**

In addition, TLD registries and domain name registration service providers must develop and implement policies and procedures to guarantee the accuracy and completeness of the information in their databases. These policies and procedures must be accessible to the public. Furthermore, non-personal domain name registration data should be made publicly available promptly after domain name registrations.

Under EU law, legitimate access seekers should also be granted access to specific domain name registration data upon submitting lawful and substantiated requests. TLD registries and domain name registration service providers must respond to such requests within 72 hours. The policies and procedures concerning data disclosure must be publicly available as well.

Finally, Article 28(6) underscores the need for compliance with the article's obligations without resulting in the duplication of domain name registration data collection. TLD registries and domain name registration service providers must collaborate and prevent duplication.

Navigating the ambiguity of the NIS2 Directive in the domain industry

The NIS2 Directive has generated significant concerns among domain professionals. While its primary goal is to strengthen cybersecurity and bolster infrastructure resilience across the EU, it inadvertently places a burden on domain registries and registrars. Compliance with the Directive involves navigating a complex web of reporting requirements, stringent security measures and potential legal ramifications.

The NIS2 Directive's ambiguity has left domain experts grappling with multiple challenges, particularly regarding the verification process and responsibility allocation between registrars and registries. As the Directive aims to enhance cybersecurity, it demands stringent verification processes for domain registrations. However, the lack of clarity regarding specific procedures and standards leaves many domain professionals in the dark, forcing them to seek more concise guidelines. Additionally, the Directive does not explicitly define the roles and responsibilities of registries and registrars. This omission leads to confusion and disagreements over liability and obligations.

Amidst this turmoil, the domain industry remains vigilant, closely monitoring the situation and collaborating with key players to shape the debate. By pooling resources and expertise, the aim is to facilitate the smooth implementation of the national law in the member state, ensuring that all stakeholders can successfully navigate the intricacies of the NIS2 Directive with confidence.



The impact of NIS2 on European ccTLD registries

The NIS2 Directive introduces several crucial changes for the domain industry and TLD operators. The Directive highlights the significance of the DNS in the digital society and classifies registries as "essential entities". It places several obligations on them, such as securing their systems against security incidents and reporting them to the authorities. In the past, identifying “operators of essential services” in key areas like the digital infrastructure was left to each EU Member State. This led to an uneven application of the first NIS Directive throughout the EU. Nevertheless, almost all EU Member States identified their ccTLD registry as “operators of essential services” recognizing their crucial role in the digital infrastructure.



Polina Malaja
Policy Director, CENTR



NIS2 applies to all TLD registries operating within the EU, regardless of where they are established. It also introduces a new domain registration data accuracy obligation for TLD registries, registrars, privacy/proxy services and resellers for the purposes of DNS security. Under this obligation:

1. TLD registries and registrars must collect and maintain accurate and complete domain name registration data, including the registrant’s personal information.
2. This data must be verified.
3. TLD registries and registrars must cooperate to prevent the duplicate collection of registration data.

The practical implications of these obligations will vary based on how each EU member state incorporates the new law into their national jurisdictions.

How are European ccTLDs tackling the data accuracy requirements?

European ccTLDs already implement various data accuracy practices based on local requirements, restrictions and the availability of specific data sets. These practices also depend on the digital maturity of their national electronic identification (eID) infrastructure, local payment services and market conditions. The NIS2 Directive may cause further fragmentation and potentially increase the administrative burden on TLD registries and registrars operating in the EU. NIS2 requires additional clarification at the member state level to support cybersecurity in Europe without hindering the provision of essential digital infrastructure. Here are two aspects that need further clarification and possible solutions.

1 Concerns about verification procedures

The NIS2 Directive threatens general verification procedures, which may conflict with existing data protection obligations, such as the GDPR's data minimization principle. Verification procedures often require the collection of more data to confirm the authenticity of registration data, such as identification documents or eID data. However, without consistent and easy-to-use eID schemes throughout the EU, the domain name registration process might become more expensive and result in unnecessary delays. This could impact the European domain name industry and other sectors relying on domain names, such as e-government services and e-commerce.

To support proportionate verification procedures, EU member states should avoid blanket general verification obligations and adopt a risk-based approach. Individual ccTLD operators should be able to calculate each risk based on their needs and available resources. This approach also makes it more sustainable for registrars, as they only need to comply with a minimal set of accuracy procedures and can share the additional burden with TLD operators.

2 Lack of clarity regarding double data collection

The NIS2 Directive includes an obligation for TLD operators and registrars to prevent the duplicate registration data collection. At first glance, this supports a thin-registry business model, shifting the responsibility for data accuracy to registrars. Avoiding duplication requires placing data collection and verification responsibility on one entity rather than allowing flexible arrangements between operators. This may lead to the consolidation of registrar businesses, as identity verification can consume high levels of both time and resources. The impact of this obligation on data controller-processor relationships between TLD registries and registrars remains unclear. In order to preserve the diversity of the European domain industry,
EU member states are encouraged to allow flexible data transfer arrangements when addressing this obligation.

The NIS2 Directive aims to ensure the availability of accurate WHOIS information. However, we believe NIS2 needs more clarity at the national level to avoid disrupting existing and efficient data accuracy practices among European ccTLDs. EU member states should navigate this space carefully when implementing NIS2 requirements into their national laws to maintain the competitiveness of the European domain industry.



The challenges of the NIS2 Directive for the domain industry

The NIS2 Directive aims to enhance cybersecurity within the European Union (EU) and it holds considerable implications for domain name registrations. The first of the challenges posed by NIS2 is its nature as a directive, which necessitates transposition into national law. This process may result in market fragmentation within the domain industry if national lawmakers establish divergent requirements. As the domain industry comprises a global ecosystem of domain name registries, registrars, resellers and other stakeholders, maintaining the existing domain name lifecycle would benefit companies and customers alike.

The NIS2 Directive outlines cybersecurity measures that companies within its scope must implement. However, Article 28 is special in that it exclusively affects registries and "entities providing domain name registration services," such as registrars, resellers or other agents like privacy and proxy services, regardless of their size. Moreover, NIS2 may apply to companies outside the EU if they provide services to customers within the EU. Article 28 of NIS2 has generated considerable debate and uncertainty. It mandates that affected entities maintain a database of registration data containing specific data elements, validate data to ensure accuracy, publish non-personal data, respond to disclosure requests within 72 hours and grant access to specific domain name registration data for legitimate access seekers.



Thomas Rickert
Director at eco,
Association of the
Internet Industry

Minimum requirements should not go beyond Article 28

It would be particularly helpful if national laws establish minimum requirements that do not exceed those outlined in Article 28 and remain neutral to specific technologies and business models to minimize the risk of market fragmentation. For instance, it would be beneficial to avoid imposing specific performance requirements, such as pre-validation, allowing the companies involved to choose between pre- validation and post-validation. For example, some European ccTLDs adhere to stringent vetting procedures. However, these standards are not applicable globally. Consequently, some existing mechanisms employed for TLDs with limited geographic reach may not be suitable for use with gTLDs.



Allocation of tasks & data minimization

Various models are utilized within the domain industry to offer domain name registrations. Not only do ccTLDs and gTLDs operate differently, but there are also distinct configurations within these two categories. For registries, the following scenarios can be observed:

- Some registries maintain direct contractual relationships with registrants and therefore store all registration data in their databases.
- Some registries enforce eligibility or nexus requirements for registrants and consequently receive registration data from registrars.
- Some registries have no direct relationship with data subjects and only receive limited technical data from registrars, which is essential for operating the registry's provisioning and resolution functions. In these cases, registries have no purpose for obtaining and holding registrant data.

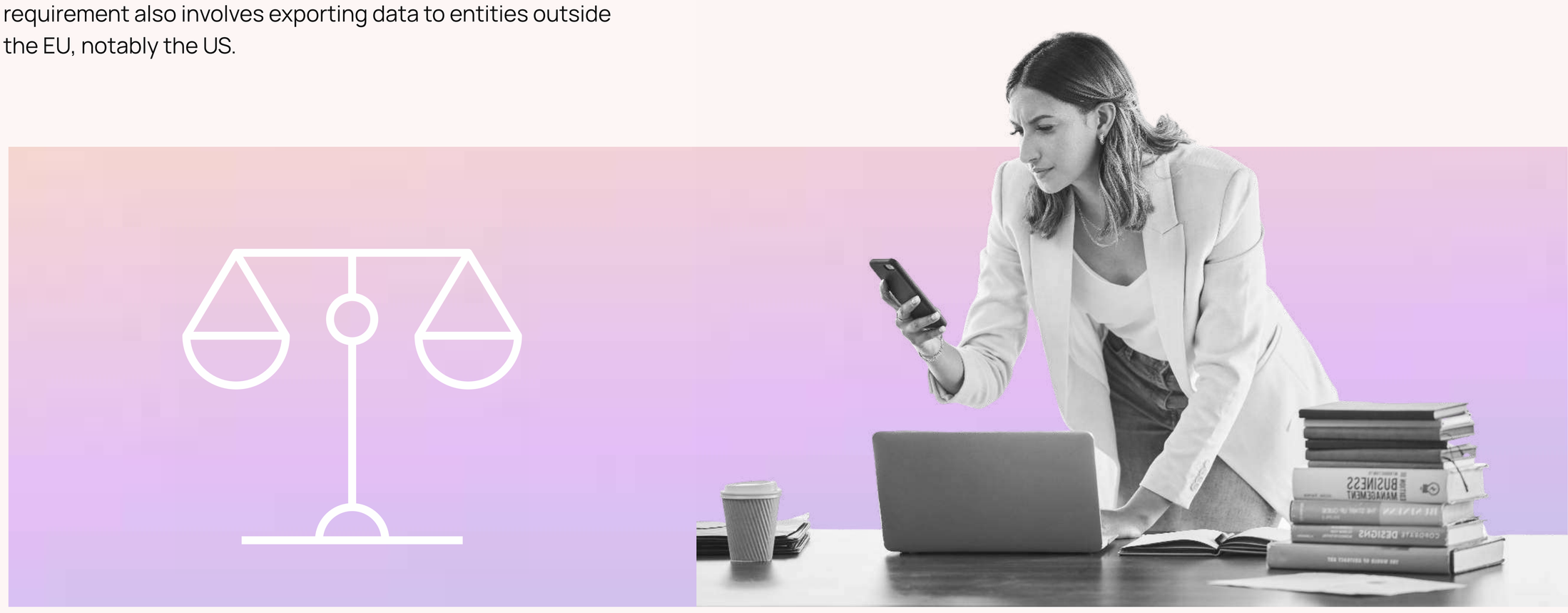
When it comes to domain name registrars or resellers, these organizations are often small. This is particularly true for ccTLD registrars and resellers (or resellers of resellers). A significant number of such entities manage fewer than 50 domain names.

Article 28 mandates that TLD registries and entities offering domain name registrations perform various tasks, as detailed in Art. 28 (1) - (5) – namely maintaining a registration database, verifying registration data, providing a public WHOIS service and processing requests for disclosure. Art. 28 (6) specifies that there should be no duplication of collection and that registries and entities providing domain name registration services must cooperate with each other.

This clause potentially leaves room for the interpretation that all entities involved in a domain name registration – such as the registry, registrar, reseller 1, and reseller 2 (sub-reseller) – must perform all tasks except for collection. This interpretation could result in multiple databases operated by numerous entities, all conducting the same processing activities, including validation of registration data, provision of public WHOIS and handling of disclosure requests. In many cases, this requirement also involves exporting data to entities outside the EU, notably the US.

The eco association believes that this is not intended to be the default situation and recommends requiring only one entity to process the same data, provided that agreements exist between them concerning the division of tasks. Such agreements would fulfill the legal cooperation requirement in Article 28 (6).

For example, a ccTLD registry with numerous registrars may opt to perform all tasks listed in Art. 28 and incorporate them into agreements with registrars. Conversely, a gTLD registry with no purpose for processing registry data may choose to have tasks performed by registrars who maintain the customer relationship and appropriately address the allocation of responsibilities in their agreements. This approach also respects the principle of data minimization, which is applied to the fullest extent possible.



The challenges of legal entity data

During the EPDP discussions at ICANN, the issue of handling the data of legal entities was a major issue. NIS2 requires operators to disclose this data, but with the caveat that it must not be published if it contains personal information. This makes it difficult for operators to achieve legal certainty. One possible solution is to allow public WHOIS service operators to publish legal entity data without risks by eliminating the need to verify whether it contains personal data.
Another challenge is the expectation that registrant email addresses should be made public unless they contain personal information. Since machines cannot determine whether an address belongs to a natural person, this verification must be done manually during the registration process for legal entities.

We believe that, when implementing the NIS2 Directive at the national level, governments should clearly understand that they should only cover the minimum requirements.

Finding the balance between legitimate access and data privacy

The NIS2 Directive requires domain name registries to provide access to information when they receive lawful and valid requests from legitimate access seekers. They must respond within 72 hours. Deciding whether or not to disclose data can be difficult, especially when balancing the interests of the access seeker and the affected data subject. It would be helpful if the European Commission could provide guidance on this in order to minimize the risk of unlawful disclosure for the involved entities. A coordination group comprising representatives from EU Member States has formed two task forces. One focuses on the issue of validation while the other works on the question of identifying legitimate access seekers. Eco has offered to collaborate with the coordination group to share the expertise of its members, to contribute to the discussions and potentially develop guidelines. The transposition must be completed by October 2024. The association is eager and prepared to assist the industry in facing this challenge.

Meeting NIS2 Directive challenges for digital infrastructure operators

The NIS2 Directive presents a series of challenges for digital infrastructure operators, as they are required to adhere to elevated cybersecurity and risk management standards. Though many companies should already have implemented these measures, the Directive introduces additional processes and attack recognition protocols. Achieving NIS2 compliance could necessitate other security measures and procedures to attain a high security standard – a hurdle for medium-sized organizations with limited resources.
For example, NIS2 creates a framework for alerting national authorities and concerned customers about cyber incidents with considerable effects on operations, financial damage or physical systems. When a major incident occurs, affected organizations must submit a preliminary report within 24 hours – a formidable challenge to their reporting abilities. Subsequently, they must also provide an in-depth report within 72 hours, followed by an extensive report within a month. Nevertheless, some operators should be well-equipped to navigate these complexities if they have high security standards.



InterNetX

InterNetX is well-prepared for the NIS2 cybersecurity requirements, primarily due to its ISO-27001 certification of DNS services including associated network and IT infrastructure. This certification demonstrates the company's commitment to maintaining the highest information security and management standards.

Checklist →

Checklist for the NIS2 Directive

By following this checklist, you can ensure that your business is well positioned to comply with the NIS2 Directive and effectively manage cybersecurity risks.

1 Familiarize yourself with the NIS2 Directive

- ☐ Review the NIS2 Directive and its objectives
- ☐ Understand the key changes in comparison to NIS1

2 Identify your organization's role

- ☐ Determine under which sector and entities your organization falls
- ☐ Analyze the specific obligations and requirements for your sector and entity

3 Assess risk management capabilities

- ☐ Evaluate your organization's current risk management framework
- ☐ Identify areas for improvement and alignment with NIS2 Directive requirements

4 Implement security measures

- ☐ Develop a comprehensive cybersecurity strategy, incorporating NIS2 Directive guidelines
- ☐ Implement appropriate technical and organizational measures to address identified risks
- ☐ Regularly review and update security measures based on evolving threats

5 Establish incident reporting procedures

- ☐ Create a robust incident response plan, including reporting obligations under NIS2 Directive
- ☐ Appoint a dedicated team to handle incident reporting and coordination with relevant authorities
- ☐ Ensure mandatory reporting timelines are met in case of a security incident

6 Engage with Competent Authorities and CSIRTs:

- ☐ Identify the relevant national Competent Authority and Computer Security Incident Response Team (CSIRT) for your organization
- ☐ Establish communication channels and share relevant information regarding security incidents

7 Conduct regular audits and assessments

- ☐ Implement a schedule for periodic internal and external audits to ensure compliance with NIS2 Directive
- ☐ Address any identified gaps or shortcomings in your organization's cybersecurity posture

8 Staff training and awareness

- ☐ Provide regular training sessions for employees to raise awareness about cybersecurity best practices and NIS2 Directive
- ☐ Encourage a strong security culture within the organization

9 Supply chain security

- ☐ Assess the cybersecurity posture of third-party suppliers and partners
- ☐ Implement contractual obligations and security standards for supply chain entities

10 Monitor national implementation updates

- ☐ Stay informed on updates to the NIS2 Directive and related national regulations
- ☐ Adjust your organization's cybersecurity strategy and practices accordingly to re-main compliant

Conclusion. INTERNETX is your ally in tackling NIS2 challenges and beyond

As this e-paper comes to its conclusion, it is clear that the NIS2 Directive represents a significant step forward in the European Union's efforts to bolster the cybersecurity of its digital infrastructure. While the process of transposition and implementation is still ongoing, with many details yet to be ironed out, the focus on harmonization, enhanced security measures and collaboration among member states send a strong message about the EU's commitment to a secure and resilient digital future.

For digital infrastructure operators and domain experts, the NIS2 Directive presents both challenges and opportunities. As sector-specific schemes for certifying compliance are developed, organizations must stay informed and proactive in navigating this evolving landscape. By aligning themselves to globally established best practices for cybersecurity, organizations can work towards achieving compliance and enhancing their overall security posture.

Navigating the future of NIS2

As we look to the future, it is essential to recognize that digital transformation and cybersecurity are inextricably linked. The NIS2 Directive reminds us of the need for innovation and resilience in our digital world. By embracing modern IT infra-structures, secure-by-default hardware and software, zero trust architecture, and customer-managed encryption tools, organizations can ensure they are well-positioned to thrive in this rapidly changing environment.

Finally, the successful implementation of the NIS2 Directive will require collaboration and partnership among all stakeholders, including industry leaders, lawmakers and national cybersecurity authorities. By working together to create a robust and secure digital ecosystem, we can protect the interests of citizens, businesses and governments.

As digital operators and domain professionals, it's essential to reflect on advancing your cybersecurity capabilities from a basic understanding to a more sophisticated level. Strengthening your defense and reliability with all-encompassing solutions for cybersecurity risk and incident reporting measures is essential, particularly in protecting critical assets like servers, domain names and DNS infrastructure.

The arrival of NIS2 has broadened the range of cybersecurity risk management and governance requirements, directly impacting our industry. The existing gap in security, especially in operational cybersecurity, necessitates deploying efficient, integrated and automated solutions across working environments. Our team at InterNetX is committed to supporting you with our expertise, helping you tailor these solutions to various risk scenarios and your organization's specific needs, including servers, domain and DNS management.

Navigating the intricacies of NIS2 together, we can help to bolster your cybersecurity resilience and position your business for ongoing success in the dynamic world of digital operations. This e-paper has provided valuable insights and guidance for your journey toward enhanced cybersecurity in the NIS2 era, equipping you with the knowledge to safeguard your digital assets and infrastructure effectively.



About.

With more than 4 million domains under management, InterNetX is one of the leading providers of white-label hosting and domain products. The domain experts provide ISPs, telecoms and agencies with domains, shared & dedicated hosting products, security solutions and network connectivity, as well as TLS/SSL and S/MIME products from all relevant CAs.

Author



By delivering compelling and technically savvy content on InterNetX's blog and diverse media, Simone contributes towards improving the shared understanding of domains and the broad internet ecosystem, nurturing a culture of information aligned towards the future.

Simone Catania - Global Content and Communications Manager

InterNetX

Johanna-Dachs-Str. 55
93055 Regensburg
Germany
Phone +49 941 59559-0
Fax +49 941 59559-55
Email: info@internetx.com
www.internetx.com

Explore our Content Hub

SNAP SHOT

Follow us

InterNetX