TaylorWessing

EU Network and Information Systems Directive 2022 (NIS2)

Purpose

NIS2 aims to build resilience to cyber threats and ensure that citizens and businesses benefit from trustworthy digital technologies. It also outlines plans to work with partners around the world to ensure international security and stability in cyberspace. NIS2 focuses on the resilience of all connected services, products and cyber communities.

Scope

Applies to public or private entities, including medium-sized enterprises, that provide their services or carry out activities within the Union, regardless of whether they fall within the medium-sized enterprise category or exceed the associated ceilings. The scope of his law is still unclear and far-reaching.

Application

In force since 16 January 2023, (replaced the 2016 NIS Directive). Fully applicable from 17 October 2024.

Operators and sectors	NIS2 identifies two groups of entities — essential and important — that provide critical services across eighteen sectors, regulated based on size. Essential Entities are large entities in eleven sectors listed in Annex I, with some specific exceptions. Important Entities include large and medium entities in seven sectors set out in Annex II and some from Annex I. The distinction between essential and important entities primarily pertains to the scope of government oversight and sanctions. National laws may differ slightly from the EU definitions.
Thresholds and exclusions	NIS2 applies to medium and large enterprises in the eighteen sectors, as defined by Commission Recommendation 2003/361/EC. Large enterprises have ≥ 250 employees, > €50 million in turnover, or > €43 million in balance sheet total. Medium enterprises have < 250 employees, ≤ €50 million in turnover, or ≤ €43 million in balance sheet total. Small enterprises, with < 50 employees and ≤ €10 million in turnover or balance sheet total, are not regulated. NIS2 does not apply to micro enterprises with fewer than ten employees and ≤ €2 million in turnover or balance sheet total, or small enterprises with fewer than 50 employees and ≤ €10 million in turnover or balance sheet total.
Sectors	NIS2 covers eighteen sectors set out in Annex I and II. **Essential sectors** include energy, transport, banking, financial markets, health, drinking water, wastewater, digital infrastructure, public administration, and space. **Important sectors** include postal and courier services, waste management, chemicals, food production, manufacturing, digital services, and research. National implementation may vary slightly from the EU sector definitions.
Essential entities	In addition to large entities in Annex I sectors, certain entities are regulated as essential regardless of size, including digital infrastructure, qualified trust service providers, TLD registries, domain registrars, medium-sized electronic communication providers, and critical public administrations. Member States may designate additional essential entities based on their significance to society and the economy.
Important entities	Important entities include large and medium entities in Annex II sectors and certain Annex I sectors. Member States can designate additional important entities based on their criticality to national or regional importance.
Cyber security requirements	NIS2 sets minimum cybersecurity requirements for essential and important entities, holding management accountable under national laws. Entities must implement comprehensive cybersecurity measures to protect IT and network services, including risk and information security policies, incident management, business continuity, supply chain security, and secure procurement practices. They must ensure the effectiveness of these measures through proper evaluation, provide cybersecurity hygiene training, and employ cryptography and encryption where possible. Additionally, measures must include personnel security, access control, asset management, multi-factor authentication, secure communication, and emergency communication systems, adopting an "all hazards approach." The EU Commission can specify requirements through implementing acts for internet providers and other sectors and define significant incidents and reporting thresholds. Cybersecurity measures should align with international and European standards, with further regulations from the EU Commission and potential mandatory use of EU cybersecurity certifications. Entities must promptly report significant disruptions, incidents, and cyber threats to national cybersecurity authorities and, where possible, inform affected service recipients. Member States should facilitate information sharing between entities with appropriate rules, platforms, and technologies. Operators of digital services and infrastructures must register with ENISA, which will inform national authorities.
National oversight	NIS2 establishes extensive requirements for national supervisory authorities and governance for cybersecurity in Member States, allowing them to exceed NIS2 requirements with their own regulations. Existing sector-specific regulations will remain if equivalent; otherwise, missing sectors must be covered by NIS2 regulations. By April 2025, Member States must compile and report lists of entities providing important and essential services to the EU Commission. Each Member State must define and implement a national cybersecurity strategy (NCSS) as the regulatory framework, including various national plans and improvements. Member States are required to designate and empower national authorities for cybersecurity tasks. These include a Competent Authority responsible for cybersecurity and oversight, a crisis management authority for handling large-scale incidents, and a national Computer Security Incident Response Team (CSIRT) for critical sectors. National cooperation between cybersecurity authorities, CSIRTs, and Single Points of Contact (SPOCs) is mandated. The German Federal Office for Information Security (BSI) serves as Germany's NIS2 Competent Authority. NIS2 mandates extensive national oversight, with detailed powers and enforcement actions for essential entities, including evidence collection, audits, security scans, and non-compliance directives. Authorities can impose operational deadlines and revoke licences for ongoing non-compliance, and management can be held personally liable for violations. Oversight for important entities is similar but slightly less stringent. For violations of NIS2 requirements, national penalties, fines, and sanctions apply, with fines up to €10 million or 2% of global turnover for ssential sectors, and up to €7 million or 1.4% of global turnover for important sectors. Member States must establish a national CSIRT to manage cybersecurity incidents, covering critical sectors, monitoring threats, issuing warnings, managing incidents, and scanning networks. National CSIRTs must be involved in incident reporting and coordinate with SPOCs in cross-border incidents. Member States must collect registration data from TLD and domain registries, including domain names and registrant contact details, with strict rules for data collection and updates within the registries.
Security incident reporting requirements	Entities subject to NIS2 must report significant security incidents to national authorities. The EU Commission's draft Implementing Act (June 2024) deems an incident significant if it meets one of eight criteria, such as causing financial losses over €100,000 or 5% of annual turnover. Losses include IT replacement, personnel costs, fines, lost revenue, consulting fees, forensic services, and ransom payments. Initial reports must be submitted within 24 hours. Incidents causing substantial reputational damage, serious health damage, death, disclosure of trade secrets, or unauthorised network access are also significant. Multiple incidents with the same root cause within six months are collectively significant. Severe operational disruptions for specific entities, such as cloud service outages over ten minutes or unmet service agreements affecting over 5% or one million EU customers for more than an hour, must be reported. Data breaches linked to malicious acts and physical access compromises to data centres must also be reported.