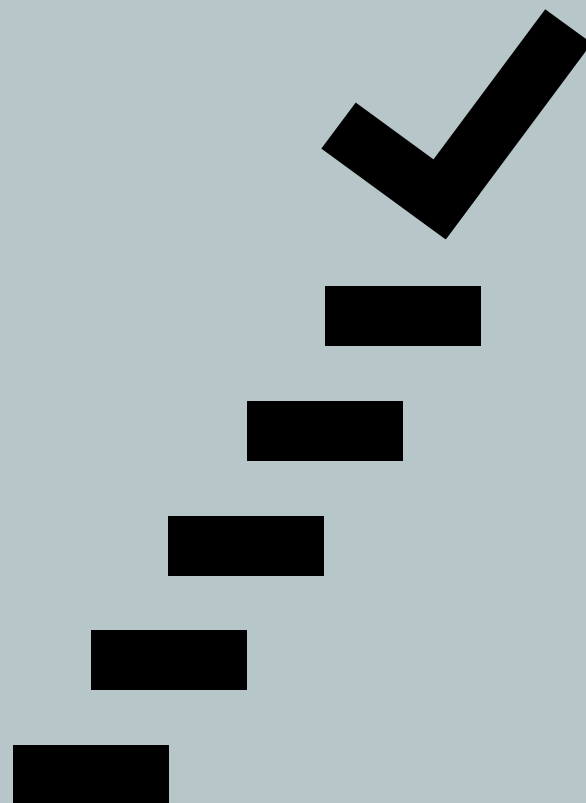


WHITEPAPER

Implementing NIS2 across Europe

A country-by-country compliance guide
for industrial sectors





About Secomea

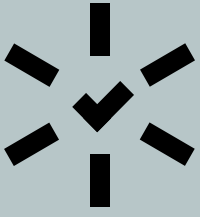
Secomea is a Secure Remote Access (SRA) solution purpose-built for operational environments and cyber-physical systems (CPS).

Over 8,000 customers around the world use it every day across thousands of sites to manage remote access to industrial equipment, reduce cybersecurity risks, and prevent downtime.

© Secomea 2025, All rights reserved. The content provided in this publication is intended for general informational purposes only and is not to be relied upon as legal or other professional advice. Although we endeavor to provide correct and timely information, we cannot guarantee its accuracy as of the date it is received, since it may not be up to date with the most recent legal or technical developments. Secomea would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. For additional information, please visit secomea.com

Table of Contents

01	Executive summary	4
02	NIS2 Directive: a brief recap.....	6
03	NIS2 implementation status across countries.....	11
04	EU-wide patterns and implementation themes.....	14
05	Country-by-country snapshot.....	16
06	How Secomea supports you in achieving NIS2 compliance.....	25



01

Executive summary

The EU's NIS2 Directive marks a major shift in how cybersecurity is governed across essential and important sectors – from energy, water, and transport to digital infrastructure and public administration – including machine vendors and manufacturers in food and beverage, chemicals, medical devices, pharmaceutical products, automotive vehicles and transport equipment, electronics, machinery, etc.

NIS2 is a EU Directive. Unlike EU Regulations (such as the GDPR) which directly apply to Member States, Directives' requirements

must be implemented locally by adopting national laws.

While the NIS2 Directive itself set a clear deadline of 17 October 2024 for national transposition, implementation progress has varied significantly across the EU and EEA.

This whitepaper offers a practical, country-by-country overview of where things stand as of mid-2025 – highlighting what national laws require, how obligations differ, and what industrial companies must do to comply – and level up their security posture at the same time.

January 2023



NIS2 Directive entered into force

17 October, 2024



National transposition deadline

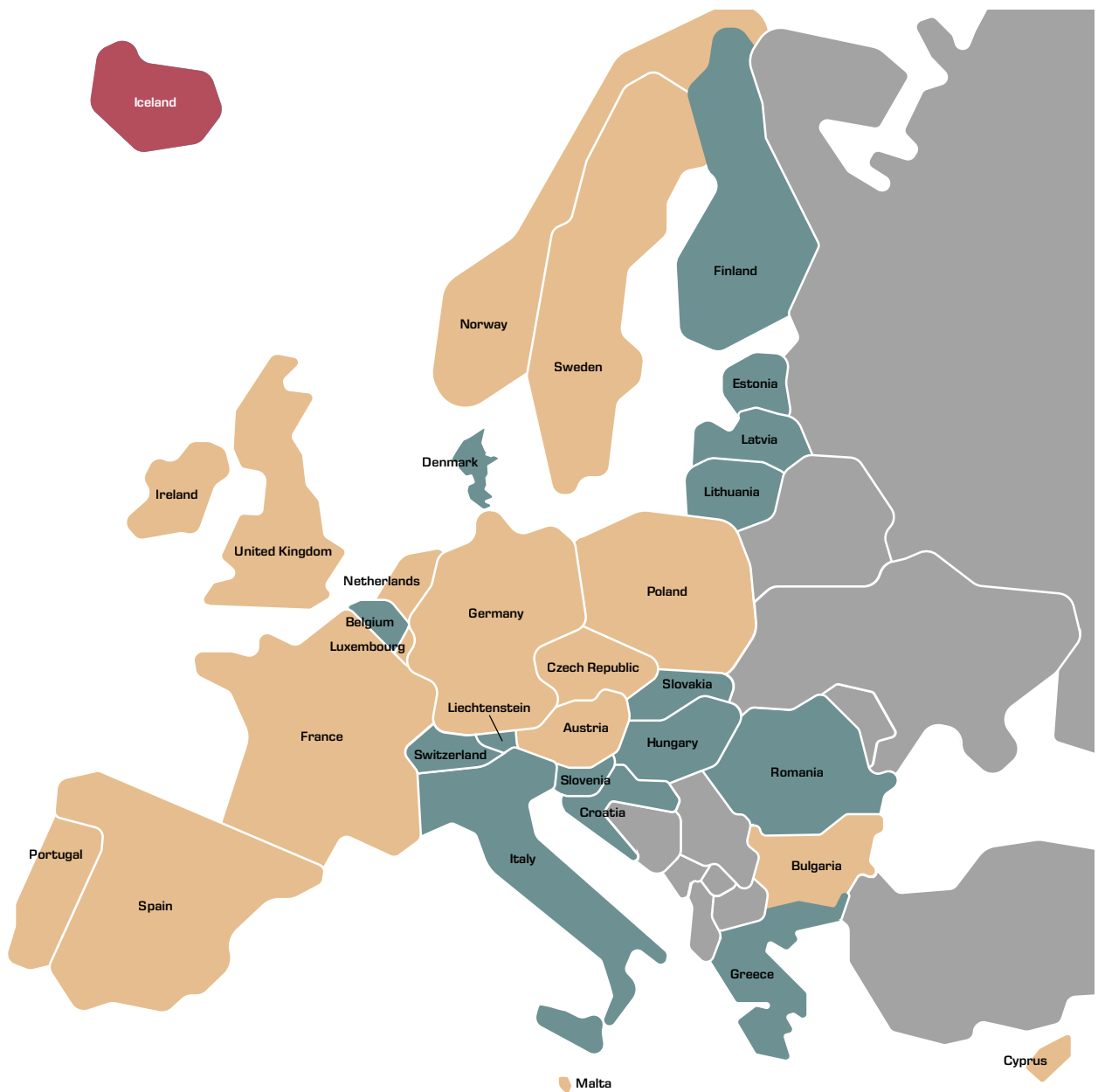
2025-2026



Country-by-country enforcement begins

NIS2 status snapshot (mid-2025)

ADOPTED	Belgium, Croatia, Denmark, Estonia, Finland, Greece, Hungary, Italy, Latvia, Liechtenstein (EEA), Lithuania, Malta, Romania, Slovakia, Slovenia, Switzerland
IN PROGRESS (draft published or consultation ongoing)	Austria, Bulgaria, Czechia, Cyprus, France, Germany, Ireland, Netherlands, Norway (EEA), Poland, Portugal, Spain, Sweden, Luxembourg, United Kingdom (non-EU/EEA)
NO DRAFT PUBLISHED / NOT YET ADOPTED	Iceland (EEA)



Key takeaways:

- **15 EU and EEA countries** have fully adopted NIS2 as of mid-2025
- Several Member States have added **stricter obligations or broadened the scope** beyond the original Directive
- **Many countries are behind schedule**, creating compliance uncertainty and legal risk for impacted entities

02

NIS2 Directive: a brief recap



What is NIS2?

What we normally refer to as NIS2 is a Directive from the European Union (2022/2555) that provides **the new EU-wide legislation on cybersecurity.**

It replaces the original NIS Directive of 2016 and aims to establish a **higher and more harmonized level of cybersecurity** across the EU and EEA – with the goal of making critical sectors more resilient to evolving cyber threats.

While the original NIS focused mainly on a handful of critical sectors and left many gaps in national enforcement, NIS2 expands both the **scope** and **stringency** of cybersecurity obligations.

Who's in scope?

The Directive applies to organizations that:

- Have **more than 50 employees** or **over €10 million in annual turnover**,

And

- Operate in **sectors** considered **critical** to societal or economic stability.

These sectors are listed in **Annex I (essential entities)** and **Annex II (important entities)** of the Directive, and include areas such as:

- Energy, water, and transport
- Health, pharmaceuticals, and medical devices
- Digital infrastructure and public administration
- Manufacturing of critical products (e.g., chemicals, electronics, machinery, vehicles).

Based on their critical importance to society, companies in these sectors are categorized as **essential** and **important** entities. The exact classification (essential vs. important) affects supervision intensity but not the core obligations.

Important entities



Research



Waste management



Manufacturing



Digital services



Postal and courier services



Industrial food processing



Chemicals manufacturing

Essential entities



Energy



Transport



Banking



Financial markets



Health & Pharma



Drinking water



Waste water



Digital infrastructure



ICT service management



Public administration



Space



	Sectors	Entities			Regime they are subject to
		< 50 employees / < € 10Mn turnover	50 employees / € 10Mn turnover	50 employees / > € 10Mn turnover	
Annex I: Sectors of high criticality	1. Energy (electricity, district heating and cooling, oil, gas and hydrogen);			✓	Essential entities
	2. Transport (air, rail, water, and road);			✓	
	3. Banking;			✓	
	4. Financial market infrastructures;			✓	
	5. Health, including entities manufacturing pharmaceutical products and preparations, as well as entities manufacturing medical devices considered to be critical during a public health emergency, like vaccines.			✓	
	6. Drinking water;			✓	
	7. Waste water;			✓	
	8. Digital infrastructure (internet exchange points; cloud computing service providers; data center service providers; content delivery networks;			✓	
	DNS service providers; TLD name registries; trust service providers;			✓	
	Qualified trust service providers and top-level TLD name registries and DNS service providers	✓			
	Providers of public electronic communications networks and publicly available electronic communications services);		✓		
	9. ICT service management: • managed service providers, providing services related to the installation, management, operation, or maintenance of ICT products, networks, infrastructure, applications, or any other network and information systems via assistance or active administration carried out either on customers' premises or remotely; • managed security service provider providing assistance for activities relating to cybersecurity risk management;			✓	
	10. Public administration			✓	
	Public administration entity at a national or regional level;	✓			
	11. Space.			✓	
Annex I & II	Entity that is the sole provider of a critical service in a Member State;	✓			Essential entities
	Entity providing a service whose disruption could have a significant impact on public safety, public security, or public health, or it could induce a significant systemic risk;	✓			
	Entity that is critical because of its specific importance at a national or regional level for the particular sector or type of service;	✓			
	Entity that is qualified as an essential entity by the national legislation implementing the Directive in the corresponding Member State.	Up to the Member State			
Annex II: other critical sectors	1. Postal and courier services;			✓	Important entities
	2. Waste management;			✓	
	3. Chemicals manufacturing;			✓	
	4. Industrial production, processing, and distribution of food			✓	
	5. Manufacturing of medical devices; computers, electronic, and optical products; electrical equipment; machinery and equipment; motor vehicles, trailers and semi-trailers; other transport equipment;			✓	
	6. Digital providers (online marketplaces, online search engines, and social networking service platforms)			✓	
	7. Research organisations			✓	

What's required?



NIS2 introduces more stringent requirements than its predecessor. The main obligations fall into three key categories:

1. Management accountability

Company leadership is explicitly responsible for ensuring compliance. They can be held **personally liable** for failures to implement or oversee required cybersecurity measures.

2. Cybersecurity measures

Organizations must implement preventive **cybersecurity measures** to mitigate the risk of cyber incidents. These **technical, operational, and organizational measures** should be **appropriate** and **proportionate** and should include at least the **10 elements listed by Article 21 of the Directive** – which are listed on the next page.

3. Incident reporting obligations

Entities must **report** incidents that can have a **significant impact on the provision of their services** to their national CSIRT or competent authority:

- Initial notification within 24 hours
- Intermediate updates as needed
- Final report within one month

The European Union Agency for Cybersecurity (ENISA) has released the NIS2 Technical Implementation Guidance, which offers practical advice on addressing NIS2 security requirements. Check it out [here](#).

10 elements to include in your cybersecurity measures

01

Policies on risk analysis and information system security

02

A plan for handling potential incidents

03

Business continuity, such as backup management, disaster recovery, and crisis management

04

Supply chain security, taking into account the vulnerabilities specific to each direct supplier and service provider

05

Security in network and information systems acquisition, development, and maintenance - including vulnerability handling and disclosure

06

Policies and procedures to assess the effectiveness of cybersecurity risk-management measures

07

Basic cyber hygiene practices and cybersecurity training

08

Policies and procedures regarding the use of cryptography and, where appropriate, encryption

09

Human resources security, access control policies, and asset management

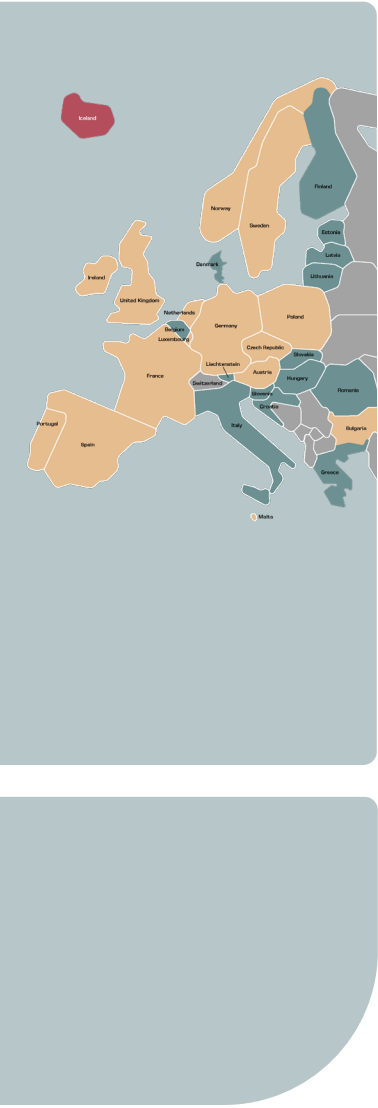


10

The use of multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications, and secured emergency communication systems within the entity, where appropriate

03

NIS2 implementation status across countries



EU	Country	Implementation status and timeline	
	AT Austria		In progress – New draft of NISG expected summer 2025; adoption likely Q3-Q4 2025
	BE Belgium		Adopted – Law passed April 2024; Royal Decree issued June; in force 18 October 2024; audit deadlines vary (5-30 months)
	BG Bulgaria		In progress – Draft amendments tabled July 2024; slowed by early elections; adoption expected late 2025
	HR Croatia		Adopted – Cybersecurity Act effective 15 February 2024; full compliance by Feb 2025-2026 depending on entity type
	CY Cyprus		In progress – Draft amendments to 2020 law expected by late 2025; enforcement likely in 2026
	CZ Czechia		Adopted – Approved April 2025; entry into force expected Q3-Q4 2025 (3 months post-publication)
	DK Denmark		Adopted – General Act in force 1 July 2025; telecom, energy, and finance laws follow with staggered entry dates into 2025-2026
	EE Estonia		Adopted – Amended Cybersecurity Act enters into force 1 July 2025
	FI Finland		Adopted – Cybersecurity Act 124/2025 in force since 8 April 2025
	FR France		In progress – Draft law submitted; expected adoption late 2025; enforcement from Q1-Q2 2026
	DE Germany		In progress – Draft published July 2024; expected adoption Q3-Q4 2025; enforcement in early 2026
	GR Greece		Adopted – Law 5160/2024 effective 27 November 2024
	HU Hungary		Adopted – Cybersecurity Act in force since 1 January 2025
	IS Iceland (EEA)		Not yet adopted – No draft published; transposition unlikely before 2026

	IE	Ireland		In progress – General Scheme published August 2024; approval delayed by elections; enforcement likely mid-2026
	IT	Italy		Adopted – Legislative Decree 138/2024 in force since 26 October 2024
	LV	Latvia		Adopted – Cybersecurity Law 2024 in force since 1 September 2024
	LI	Liechtenstein (EEA)		Adopted – Cybersecurity Law (CSG) and Decree (CSV) in force since 1 February 2025
	LT	Lithuania		Adopted – Law XII 1428/2024 in force since 18 October 2024
	LU	Luxembourg		In progress – Draft bill 8364 under review; adoption expected late 2025; enforcement in 2026
	MT	Malta		Adopted – Legal Notice 71 of 2025 issued April 2025; enforcement date pending Ministerial announcement
	NL	Netherlands		In progress – Draft law in preparation; adoption expected Q4 2025; enforcement likely Q1-Q2 2026
	NO	Norway (EEA)		In progress – Amendments to Digital Security Act expected Q4 2025; enforcement from 2026
	PL	Poland		In progress – Government approved draft in Q1 2025; Parliamentary vote due Q4 2025; entry into force early 2026
	PT	Portugal		In progress – Draft approved Oct 2024; stalled due to elections; resubmission expected Q3 2025; enforcement likely mid-2026
	RO	Romania		Adopted – Government Emergency Ordinance 155/2024 in force since 31 December 2024
	SK	Slovakia		Adopted – Amended Cybersecurity Act in force since 1 January 2025
	SI	Slovenia		Adopted – Information Security Act (ZInfV 1) in force as of 19 June 2025
	ES	Spain		In progress – Draft law approved by Council January 2025; Parliamentary debate Q3-Q4 2025; enforcement likely Q2-Q3 2026
	SE	Sweden		In progress – Government report SOU 2024:18 published; draft law expected late 2025; enforcement in 2026
	CH	Switzerland		Domestic alignment completed – Information Security Act (ISG) and associated Cybersecurity Ordinance (CSO) in force as of April 2025
	GB	United Kingdom		In progress – Not transposing NIS2; own Cyber Security and Resilience Bill in development; draft due late 2025/early 2026; enforcement expected in 2027

04

EU-wide patterns and implementation themes

As of mid-2025, the implementation of NIS2 across the EU and EEA countries is beginning to take clearer shape. While all countries are bound by the same Directive, the national transposition laws reveal both consistent patterns and meaningful divergences that industrial organizations operating across borders should be aware of.

Common patterns across Member States

Despite local differences, several themes recur in nearly all national implementations:

- **Sector coverage follows NIS2 Annex I & II**

Most countries closely mirror the Directive's sectoral scope, covering essential sectors (Annex I – e.g., energy, transport, banking, digital infrastructure, public administration) and important sectors (Annex II – e.g., manufacturing, postal services, chemicals, food, waste management). **Manufacturing and industrial operators**, especially those in OT-heavy sectors, are now firmly in scope across almost all Member States.

- **Similar registration and incident reporting models**

While registration deadlines vary, most countries require in-scope entities to register with authorities between **Q3 and Q4 2025**. Incident notification obligations

often follow the NIS2-standard model: **initial notification within 24 hours** of becoming aware of an incident, followed by **updates and a final report within 72 hours** or as information becomes available.

- **Fines align with EU thresholds**

Nearly all countries align their penalty regimes with NIS2 maximums:

- ◊ Up to **€10 million or 2%** of global annual turnover for essential entities
- ◊ Up to **€7 million or 1.4%** for important entities

Some countries, such as Poland and Malta, are introducing executive liability, enhanced audit rights, or corrective enforcement powers that **exceed the Directive's minimum requirements**.

National divergences and local interpretations

While harmonization is the goal, national implementations reflect political priorities, regulatory contexts, administrative traditions, and sector-specific cybersecurity maturity. Notable divergences include:

- **Stricter national models**
Countries like **Italy, Belgium, Hungary, Poland, and Romania** have gone beyond the Directive's baseline in several ways:
 - ◊ **Inclusion of public-sector entities**, such as municipalities, public healthcare institutions, and education providers (e.g., Italy and Romania).
 - ◊ **Mandatory internal or third-party cybersecurity audits** on a regular basis (e.g., Poland requires biennial audits, Belgium introduced ISO-aligned self-assessments).
 - ◊ **Phased compliance timelines** based on sector or entity type (e.g., Italy allows different enforcement dates per sector and entity type, in some cases into 2026).
 - ◊ **National classification systems** that replace or supplement NIS2's "essential" and "important" labels with local risk-based scoring (e.g., Hungary's national risk register)
- **Delayed or minimal progress:**
Iceland stands out as the only EEA country yet to publish a draft or initiate formal public consultation. As of June 2025, its timeline remains unclear, and transposition is unlikely before 2026.
- **Different enforcement structures**
Enforcement authority varies widely:
 - ◊ **Centralized models** – Some countries centralize supervision and enforcement under a **national cybersecurity authority**. Countries like **Finland (Traficom), Lithuania (NCSC), and Malta (MITA/CIPD)** rely on one primary agency.
 - ◊ **Decentralized models** – Others use a **sectoral approach**, distributing enforcement responsibility across industry-specific regulators – often coordinated by a central agency (e.g., Italy's ACN works with sector ministries; Slovakia assigns tasks to sector-specific bodies under the National Security Authority).
- **Unique national adaptations:**
Some countries are leveraging NIS2 to consolidate or align overlapping cybersecurity laws:
 - ◊ **France** is bundling NIS2, DORA, and CER into a single Resilience Act
 - ◊ **Germany** is integrating NIS2 into its broader **KRITIS** regime for critical infrastructure
 - ◊ The **Netherlands** and **Sweden** are emphasizing multi-stakeholder governance and proposing detailed models for **supply chain security and collaborative incident response**.



Implications for OT-heavy and industrial sectors operating across borders

For manufacturers, utilities, and other industrial operators, these trends and variations mean that while the **core obligations are broadly similar across Europe**, the level of regulatory maturity, enforcement intensity, and sectoral complexity will vary across jurisdictions.

Companies operating in multiple countries must adapt to differences in:

- Whether **public institutions** are in scope
- **Registration and compliance deadlines** by country and sector
- **Audit and reporting requirements**, especially where stricter than originally dictated

by the NIS2 Directive

- Which **authorities** are responsible for oversight and enforcement.

These discrepancies can create challenges for multinational organizations aiming to maintain a consistent cybersecurity posture. However, they also present a strategic opportunity.

By adopting a **Zero Trust-based remote access architecture**

– featuring centralized logging, granular role-based access, and secure third-party management – organizations can build a strong foundation that satisfies both EU-wide compliance requirements and local implementation nuances.



05

Country-by-country snapshot

 AUSTRIA	
Implementation status	● In progress
Transposing legislation	Amendment to the current NISG (Netz- und Informationssystemssicherheitsgesetz 2024), often referred to as NISG 2024
Official link	/
Authority in charge	Bundesamt für Sicherheit in der Informationstechnik (BSI) and sector-specific supervisors
Deviations or additions	Integration into existing NIS1 law; national exemptions not anticipated, but certain sectors (telecom, health) may have transitional grace periods of 6 months post-enactment.
Enforcement & penalties	Penalties expected to align with NIS2 maxima
Entry into force and/or relevant timelines	The original draft for the Netz- und Informationssystemssicherheitsgesetz 2024 (NISG 2024) was rejected by Parliament on 3 July 2024, due to a lack of the required two-thirds majority. A new draft is expected in summer 2025, and full transposition is unlikely to occur before Q3-Q4 2025. Full enforcement is likely to occur in 2026, with registration deadlines approximately three months after the effective date.
 BELGIUM	
Implementation status	● Transposition completed
Transposing legislation	Law of 26 April 2024 on cybersecurity and Royal Decree
Official link	Loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique
Authority in charge	Centre for Cybersecurity Belgium (CCB)
Deviations or additions	Belgium has introduced stricter obligations for managed service providers (MSPs) and organizations in the healthcare and transportation sectors. Specific risk analysis and governance expectations exceed the NIS2 baseline in some domains. There is also a requirement for entities to report their cybersecurity officers and responsible contact points. The law is aligned with ISO 27001 and the CyberFundamentals Framework (CyFun), a cybersecurity framework developed by the Centre for Cybersecurity Belgium (CCB). It had also introduced an obligation of ISO-aligned self-assessments and a presumption of compliance for ISO 27001-certified entities.
Enforcement & penalties	Penalties aligned with NIS2 maxima, and scaling depending on entity classification
Entry into force and/or relevant timelines	The law took effect on 18 October 2024. Entities faced registration and self-assessment deadlines ranging from 5 to 30 months, depending on entity size and classification.
 BULGARIA	
Implementation status	● In progress
Transposing legislation	Draft amendments to the Cybersecurity Act 2018
Official link	/
Authority in charge	State Agency for National Security (SANS), with operational support from CERT-BG
Deviations or additions	The draft law includes sector-specific thresholds and classification criteria. Phased compliance deadlines are anticipated, though exact dates are still under negotiation.
Enforcement & penalties	The planned penalty framework is still in draft – penalties are expected to align with NIS2, but specific scales are yet to be finalized.
Entry into force and/or relevant timelines	A draft bill to amend the 2018 Cybersecurity Act was formally tabled before Parliament in September 2024, passed in its first reading on 20 February 2025, and remains pending final adoption. Final adoption is expected by Q4 2025, with enforcement scheduled for early 2026, pending legislative progress.

 CROATIA	
Implementation status	● Transposition completed
Transposing legislation	Cybersecurity Act (Zakon o kibernetičkoj sigurnosti NN 14/2024)
Official link	Zakon o kibernetičkoj sigurnosti
Authority in charge	Centre for Cybersecurity Belgium (CCB)
Deviations or additions	Croatia has introduced an extended compliance phase-in period (up to 12 months post-notification). Sector-specific rules will be further defined via secondary regulation, including technical mandates and risk assessment procedures.
Enforcement & penalties	Penalties aligned with NIS2 tiers and include senior management fines for governance failures
Entry into force and/or relevant timelines	The Cybersecurity Act entered into force on 15 February 2024, making Croatia one of the first EU countries to complete NIS2 transposition. Entities were required to register themselves by February 2025, and their compliance deadlines are within 1 year of notification (i.e., by February 2026), though implementing regulations may adjust some deadlines.
 CYPRUS	
Implementation status	● In progress
Transposing legislation	Amendments to the Security of Networks and Information Systems Act (Law 89(I)/2020)
Official link	/
Authority in charge	Digital Security Authority (DSA-CY)
Deviations or additions	The law will likely include localized thresholds and risk-based adjustments tailored to Cypriot ecosystem needs. It will also probably expand risk assessment and reporting models to accommodate public sector and national resilience goals.
Enforcement & penalties	Penalty amounts and scales have yet to be defined; secondary legislation will provide clarification.
Entry into force and/or relevant timelines	Draft law expected by late 2025 or early 2026.
 CZECHIA	
Implementation status	● Adopted (entry into force pending)
Transposing legislation	Act on Cybersecurity (final title pending Republic Gazette publication)
Official link	Act on Cybersecurity
Authority in charge	National Cyber and Information Security Agency (NÚKIB)
Deviations or additions	The Czech Act adds management liability, data localization, and detailed Supply-Chain Risk Management (SCRM), going beyond NIS2's baseline standards
Enforcement & penalties	Penalty amounts aligned to NIS2
Entry into force and/or relevant timelines	Enforcement is pending publication and will take effect three months after promulgation, likely in Q3-Q4 2025.
 DENMARK	
Implementation status	● Transposition completed
Transposing legislation	- Act No. 434 on measures to ensure a high level of cybersecurity (general NIS2 framework) – Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau – in force since 1 July, 2025. - Telecommunications Security and Preparedness Act – Lov om sikkerhed og beredskab i telesektoren – draft submitted to Parliament in February 2025, expected to be enacted in 2025 - Energy Sector Cybersecurity Act – Lov om cyber- og beredskabsstiltag i energisektoren (formal title may vary) – introduced in March 2025; executive orders and detailed guidance are currently being finalized; sector-specific measures will be implemented post-framework in 2025; final entry dates pending. Amendments incorporated into the Danish Financial Business Act - Lov om finansiel virksomhed – under Section 333, aligning it with NIS2 – already effective since early 2025.
Official link	Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau
Authority in charge	The Danish Centre for Cybersecurity (CFCS) handles overall coordination, supported by sectoral regulators: - Danish Energy Agency - Danish Financial Supervisory Authority - Danish Transport, Construction & Housing Authority (telecom)
Deviations or additions	Denmark is taking a sectoral approach rather than adopting a single unified law. This means NIS2 obligations are transposed through a general framework plus sector-specific laws. A notable deviation is the three-tier classification model for telecom operators, replacing NIS2's standard two-tier

	system to tailor requirements proportionately to provider size and risk level.
Enforcement & penalties	Penalties aligned to NIS2 minimum standards
Entry into force and/or relevant timelines	- Framework Act No. 434 is in force from 1 July 2025 - Sector-specific laws (telecom, energy, finance) follow staggered implementation, with public consultation completed or ongoing through mid-2025 - A national NIS2 strategy and contact points are available on Denmark's Digital Strategy Commission portal Although the general framework has now been adopted, Denmark's full sector-specific implementation will continue to evolve beyond Q3 2025.
🇪🇺 ESTONIA	
Implementation status	● Transposition completed
Transposing legislation	Amendment to the Cybersecurity Act
Official link	Küberturvalisuse seaduse ja teiste seaduste muutmise seadus (küberturvalisuse 2. direktiivi ülevõtmine)
Authority in charge	Estonian Information System Authority (RIA)
Deviations or additions	None disclosed yet; implementation will follow standard NIS2 phasing via Cabinet Regulations
Enforcement & penalties	Penalties aligned with the NIS2 Directive
Entry into force and/or relevant timelines	Entered into force on 1 July 2025
🇫🇮 FINLAND	
Implementation status	● Transposition completed
Transposing legislation	Cybersecurity Act 124/2025
Official link	Kyberturvallisuuslaki
Authority in charge	Ministry of Transport & Communications (LVM); supervision via Traficom/Finnish Medicines Agency (Fimea) entity registry
Deviations or additions	Finland's legislation unified the operator category: there is no distinction between essential and important entities. Compliance audits are only triggered by a serious incident occurring, the company's failure to register properly, or suspicion of non-compliance.
Enforcement & penalties	Penalties are likely to be aligned with the NIS2 Directive; however, amounts have not yet been published.
Entry into force and/or relevant timelines	Entered into force on 8 April 2025
🇫🇷 FRANCE	
Implementation status	● In progress
Transposing legislation	Projet de loi relatif à la résilience des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier (a unified law covering NIS2, CER, and DORA)
Official link	/
Authority in charge	Agence nationale de la sécurité des systèmes d'information (ANSSI)
Deviations or additions	France plans to exceed the basic NIS2 requirements by incorporating enhanced ICS/SCADA safeguards, broader coverage of local authorities (including departments, larger communes, and overseas territories), and alignment with financial resilience standards under DORA.
Enforcement & penalties	Fines expected to mirror or exceed NIS2 levels
Entry into force and/or relevant timelines	A draft law consolidating NIS2, CER, and DORA was submitted and is expected to be adopted in the second half of 2025 and enter into force from Q1-Q2 2026.
🇩🇪 GERMANY	
Implementation status	● In progress
Transposing legislation	IT-Sicherheitsgesetz 3.0 (also known as NIS2UmsuCG)
Official link	/
Authority in charge	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Deviations or additions	Germany's draft introduces increased log-retention policies, mandatory supply-chain risk assessments, and proactive monitoring – in continuation of Germany's broader KRITIS oversight regime. Critical infrastructure designation is retained alongside NIS2's essential and important categories.
Enforcement & penalties	Fines expected to mirror or exceed NIS2 levels

Entry into force and/or relevant timelines	A draft law was published in July 2024; Bundestag deliberation was delayed due to the Federal elections in February 2025. The expected transposition period is Q3-Q4 2025, with enforcement anticipated in early 2026.
 GREECE	
Implementation status	● Transposition completed
Transposing legislation	Νόμος 5160/2024
Official link	ΦΕΚ Α 195/27-11-2024
Authority in charge	National Cybersecurity Authority (NCA)
Deviations or additions	The law extends coverage to include semi-public organizations and mandates the appointment of an Information and Communication Systems Security Officer (ICSSO). Also, it includes additional requirements of maintaining a detailed asset inventory (beyond NIS2's baseline), submitting a cybersecurity policy to NCA annually, and providing swift incident triage via a three-stage reporting process (24h warning, 72h update, 30-day final report).
Enforcement & penalties	Penalties aligned with the NIS2 Directive
Entry into force and/or relevant timelines	The law entered into force on 27 November 2024. Additionally, the NCA provided technical and organizational implementation details directly through Ministerial Decisions, such as Joint Ministerial Decision 1689/2025 (JMD).
 HUNGARY	
Implementation status	● Transposition completed
Transposing legislation	Cybersecurity Act LXIX of 2024, supplemented by Government Decree 418/2024, outlining implementation details
Official link	Cybersecurity Act LXIX of 2024
Authority in charge	Supervisory Authority of Regulated Activities (SZTFH) – serving as Hungary's cybersecurity authority
Deviations or additions	Hungary introduced a security classification framework, which is a more detailed and prescriptive approach than NIS2's high-level risk management model. All entities must classify systems into "basic," "significant," or "high" security levels, with varying obligations tied to each classification. These classifications drive control requirements specific to the classified level. Hungary mandates regular audits as part of their national implementation: organizations must enter into an auditor contract within 120 days of registration and conduct their first cybersecurity audit by December 31, 2025, followed by biennial audits thereafter.
Enforcement & penalties	Penalties aligned with the NIS2 Directive
Entry into force and/or relevant timelines	1 January 2025. The first audit deadline is 31 December 2025, with audits scheduled to recur every two years.
 ICELAND (EEA)	
Implementation status	● Not yet adopted
Transposing legislation	/
Official link	/
Authority in charge	National Cybersecurity Authority (under the Ministry of Justice).
Deviations or additions	None have been identified yet; Iceland tends to follow EU standards with minor country-specific adaptations.
Enforcement & penalties	To be defined; expected to mirror NIS2 fines and national criminal/administrative regimes.
Entry into force and/or relevant timelines	Intent announced, but no draft published yet; no public timeline for transposition – but likely post 2025.
 IRELAND	
Implementation status	● In progress
Transposing legislation	National Cyber Security Bill 2024
Official link	/
Authority in charge	National Cyber Security Centre (NCSC) and dedicated sectoral regulators (e.g., Central Bank for finance, CRU for energy, ComReg for telecoms, various transport authorities, and Health agencies)
Deviations or additions	Specific legislative deviations (e.g., IT Security Officer roles, risk class hierarchies) have yet to be defined.
Enforcement & penalties	Fines expected to mirror NIS2 levels
Entry into force and/or relevant timelines	The General Scheme (outline) of the National Cyber Security Bill 2024 was published in August 2024 and is pending approval (delayed by elections); enforcement likely in mid-2026.

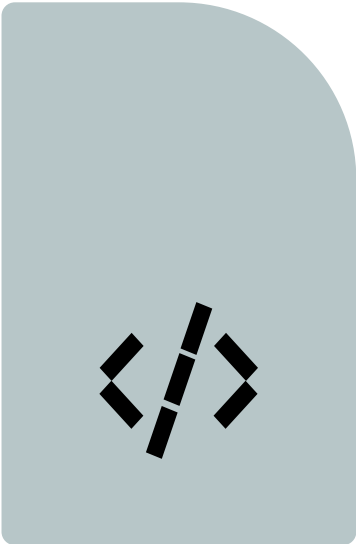
🇮🇹 ITALY	
Implementation status	● Transposition completed
Transposing legislation	Legislative Decree No. 138/2024
Official link	Decreto Legislativo 138/2024
Authority in charge	Agenzia per la Cybersicurezza Nazionale (ACN)
Deviations or additions	Italy extended the scope to public service actors, spanning 18 sector. It also introduced phased registration and compliance deadlines, and centralized oversight through the ACN's digital monitoring platform.
Enforcement & penalties	Penalties aligned with the NIS2 Directive
Entry into force and/or relevant timelines	The decree took effect on 26 October 2024. Registration and compliance followed a phased timeline: digital service providers must register between 1 December 2024 and 17 January 2025, while all other entities must register by 28 February 2025. Incident reporting obligations begin in January 2026 (approximately nine months after registration), and full implementation of governance and risk management controls is required by October 2026 (around 18 months post-registration).
🇱🇻 LATVIA	
Implementation status	● Transposition completed
Transposing legislation	Cybersecurity Law 2024
Official link	Nacionālās kiberdrošības likums
Authority in charge	National Cyber Security Centre (NCSC)
Deviations or additions	Registration follows a phased approach based on entity classification (essential vs. important). All covered entities must appoint a designated Cybersecurity Manager by 1 October 2025, responsible for conducting annual security reviews and submitting compliance reports. Secondary legal acts introduced detailed obligations for ICT infrastructure, including DNS services and data centers.
Enforcement & penalties	Penalties aligned with the NIS2 Directive
Entry into force and/or relevant timelines	The law took effect on 1 September 2024. The appointment of a cybersecurity manager and submission of a self-assessment report are due on 1 October 2025
🇱🇮 LIECHTENSTEIN (EEA)	
Implementation status	● Transposition completed
Transposing legislation	Updated Cyber Security Law (CSG), with related Cyber Security Decree (CSV), complemented by CSIRT-LI's RFC 2350 and operational guidelines
Official link	Cyber-Sicherheitsverordnung (CSV)
Authority in charge	National Cyber Security Unit (under the Government Office for National Security) and CSIRT-LI
Deviations or additions	The national legislation sets local thresholds, incident-notification procedures, and registration rules in line with NIS2 – tailored to Liechtenstein's small-state and EEA context.
Enforcement & penalties	Penalties are harmonized with NIS2 but adjusted to local legal scale (e.g., fines up to CHF 100k).
Entry into force and/or relevant timelines	1 February 2025
🇱🇹 LITHUANIA	
Implementation status	● Transposition completed
Transposing legislation	Cybersecurity Act of the Republic of Lithuania, 2024 - Law No. XII-1428/2024
Official link	Lietuvos Respublikos kibernetinio saugumo įstatymas
Authority in charge	National Cyber Security Centre (NCSC-LT)
Deviations or additions	Lithuania introduced an ex ante supervision model, including mandatory risk assessments, cyber policies, and senior management training (with a minimum frequency of every two years); it also applied domestic data-localization rules to public networks and secure state data networks.
Enforcement & penalties	Penalties aligned with the NIS2 Directive, with lower caps for public sector bodies
Entry into force and/or relevant timelines	18 October 2024

 LUXEMBOURG	
Implementation status	● In progress
Transposing legislation	Projet de loi 8364 portant adaptation du droit national à la directive NIS 2
Official link	/
Authority in charge	Luxembourg Institute of Regulation (ILR-NCIS) and CSSF (financial sector). The Haut-Commissariat à la Protection Nationale (HCPN) – Luxembourg's GOVCERT.LU – will serve as CSIRT.
Deviations or additions	None yet indicated
Enforcement & penalties	Fines expected to mirror NIS2 levels
Entry into force and/or relevant timelines	A parliamentary debate is scheduled for Q3 2025, with entry into force expected between late 2025 and early 2026.
 MALTA	
Implementation status	● Transposition completed – awaiting enforcement
Transposing legislation	Legal Notice 71 of 2025 (S.L. 460.41)
Official link	Measures for a High Common Level of Cybersecurity Across the EU (Malta) Order, 2025 (S.L. 460.41)
Authority in charge	Critical Infrastructure Protection Department (CIPD) & Malta CSIRT
Deviations or additions	Malta introduced a new policy requirement: a Coordinated Vulnerability Disclosure (CVD) framework. The local legislation also strengthened management-level liability and codified the 24-hour initial incident notification and 72-hour follow-up reporting.
Enforcement & penalties	Penalties aligned with the NIS2 Directive
Entry into force and/or relevant timelines	Adopted in April 2025; awaiting the Minister's announcement of its enforcement date.
 NETHERLANDS	
Implementation status	● In progress
Transposing legislation	Work is ongoing on a "Cybersecurity Act" – a consolidated working draft title has not yet been officially published
Official link	/
Authority in charge	National Cyber Security Centre (NCSC-NL)
Deviations or additions	Expected emphasis on multi-stakeholder risk sharing and coordinated incident management across critical supply chains.
Enforcement & penalties	Fines expected to mirror NIS2 levels
Entry into force and/or relevant timelines	Draft law adoption planned for Q3 2025, with actual enforcement likely from Q1-Q2 2026.
 NORWAY (EEA)	
Implementation status	● In progress
Transposing legislation	Amendments to Digital Security Act ("Digitalsikkerhetsloven")
Official link	/
Authority in charge	Ministry of Justice and Public Security, Norwegian National Security Authority (NSM), and sector-specific regulatory bodies
Deviations or additions	Introduction of a Coordinated Vulnerability Disclosure component for essential providers; planned emphasis on multi-stakeholder incident cooperation, particularly for OT supply chains.
Enforcement & penalties	Fines expected to mirror NIS2 levels
Entry into force and/or relevant timelines	Norway intends to amend the Digital Security Act (Digitalsikkerhetsloven); a draft has not been published yet; expected Q4 2025; enforcement likely from 2026.
 POLAND	
Implementation status	● In progress
Transposing legislation	Amendment to National Cybersecurity System Act (NCSSA)
Official link	/
Authority in charge	Ministry of Digital Affairs; sector CSIRTs under respective ministries
Deviations or additions	The amendment introduces restrictions on high-risk 5G vendors, extending beyond telecommunications to cover all NIS2-critical sectors. This means that companies in energy, transport, healthcare, and manufacturing will also be prohibited from using equipment or services from vendors flagged for national security concerns. It also mandates biennial audits and rigorous supply-chain security protocols; plus, it introduces management liability, capped at 300% of the executive's salary for non-compliance.

Enforcement & penalties	Fines align with NIS2 caps, and Poland adds a special top-tier sanction of up to PLN 100 million (about €23 million) for threats to state security or critical infrastructure.
Entry into force and/or relevant timelines	A draft amendment to the National Cybersecurity System Act (NCSSA) was published in April 2024, approved by the Government in Q1 2025, and is now pending a Parliamentary vote in Q4 2025, with expected enforcement in early 2026. Sectoral regulations and entity registries are expected to be established through Council Decrees following enactment.
 PORTUGAL	
Implementation status	 In progress
Transposing legislation	Law 46/2018 – Regime Jurídico da Cibersegurança (RJC)
Official link	/
Authority in charge	National Cybersecurity Centre (CNCS) and sectoral regulators (e.g., ANACOM for telecoms)
Deviations or additions	Proposed measures include duties for a cybersecurity officer, stronger supply-chain risk management clauses, and provisions for personal liability of directors, with fines up to €200,000 in some drafts – although this may change before final enactment.
Enforcement & penalties	To be finalized post-consultation; fines in line with EU norms
Entry into force and/or relevant timelines	A draft NIS2 transposition bill, part of a broader Regime Jurídico da Cibersegurança (RJC), was approved in October 2024 and underwent public consultation until December 2024. The bill stalled due to new elections; the proposal now awaits re-submission under a new administration, likely in Q3 2025, targeting approval by early 2026 and enforcement by mid-2026 onwards.
 ROMANIA	
Implementation status	 Transposition completed
Transposing legislation	Government Emergency Ordinance (GEO) 155/2024 on cybersecurity and incident reporting
Official link	ORDONANȚĂ DE URGENȚĂ nr. 155 din 30 decembrie 2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil
Authority in charge	DNSC (National Cyber Security Directorate)
Deviations or additions	Romania introduced clarifications on territorial scope and phased deadlines. DNSC's secondary orders will detail requirements for registration and reporting.
Enforcement & penalties	Aligned with the NIS2 Directive
Entry into force and/or relevant timelines	31 December 2024
 SLOVAKIA	
Implementation status	 Transposition completed
Transposing legislation	Amendment to Act No. 69/2018 Coll. on Cybersecurity
Official link	Act No. 69/2018 Coll. on Cybersecurity
Authority in charge	National Security Authority (NSA, also known as NBU)
Deviations or additions	Slovakia introduced detailed classification criteria (essential vs. important) listed directly in law. The amendment enforced multi-stage incident reporting, including early warning (within 24 hours), full notification (within 72 hours), as well as intermediate and final reports. It also strengthened supply-chain oversight, including contractor compliance and auditing mandates.
Enforcement & penalties	Aligned with the NIS2 Directive
Entry into force and/or relevant timelines	1 January 2025
 SLOVENIA	
Implementation status	 Transposition completed
Transposing legislation	Information Security Act
Official link	ZInfV-1
Authority in charge	Government Office for Information Security (URSIV), supported by SI-CERT and the State Administration CSIRT team, all coordinated under the National Information Security Authority
Deviations or additions	The law introduces a self-registration platform for entities, a single national incident reporting portal, clear incident reporting timelines (early warning, updates, final report), and provisions for cross-sector vulnerability and information sharing

Enforcement & penalties	Aligned with the NIS2 Directive
Entry into force and/or relevant timelines	19 June 2025
 SPAIN	
Implementation status	 In progress
Transposing legislation	Proyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad ("Coordination and Cybersecurity Governance Bill")
Official link	/
Authority in charge	Centro Criptológico Nacional (CCN-CERT), coordinating with sector regulators
Deviations or additions	The draft introduces a formal national catalog of essential and important entities, with classifications that are slightly more prescriptive than those in NIS2. It also strengthens third-party and supply chain risk requirements, mandating active oversight of shadow suppliers and the inclusion of resilience clauses in vendor contracts.
Enforcement & penalties	Fines in line with EU norms
Entry into force and/or relevant timelines	A draft law integrating NIS2, CER, and DORA-related provisions was approved by the Council in January 2025 and will undergo Parliamentary vote in Q3-Q4 2025; enforcement likely in Q2-Q3 2026.
 SWEDEN	
Implementation status	 In progress
Transposing legislation	Swedish Cybersecurity Act: Cybersäkerhetslagen
Official link	Nya regler om cybersäkerhet, SOU 2024:18
Authority in charge	The Swedish Civil Contingencies Agency (MSB) will serve as the primary Competent Authority; the Post and Telecom Authority (PTS) will oversee Digital Service Providers, and individual sector regulators will oversee Operators of Essential Services (OES)
Deviations or additions	The draft law proposes to integrate NIS2 with Sweden's national Critical Entities Resilience (CER) strategy. It's expected to introduce stricter incident reporting timelines and expanded enforcement powers for the Swedish Civil Contingencies Agency (MSB), beyond those in NIS1.
Enforcement & penalties	Administrative fines are expected to align with GDPR-levels (up to 2% of global turnover or SEK 120 million)
Entry into force and/or relevant timelines	A government report (SOU 2024:18) was published in March, and the consultation closed in late May. No draft law has been submitted to Parliament yet. Enforcement is unlikely before 2026.
 SWITZERLAND	
Implementation status	 Domestic alignment completed
Transposing legislation	Information Security Act (ISG) and associated Cybersecurity Ordinance (CSO)
Official link	Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG), Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen
Authority in charge	National Cyber Security Centre (NCSC, now BACS)
Deviations or additions	While Switzerland is not an EU/EEA member bound to transpose the NIS2 Directive, its national ISG/CSO regime mirrors many NIS2 obligations – especially around critical infrastructure. The scope includes public authorities and operators of nine critical infrastructure sectors: energy, water, transport, health, finance, ICT, public safety, supply/disposal, and food. The Information Security Act (ISG) requires organizations to ensure contractual cybersecurity compliance by third parties and service providers. Public authorities must implement comprehensive information security management systems (ISMS), staff security education, vulnerability reporting, and removal frameworks. In the event of a cybersecurity incident, the Cybersecurity Ordinance (CSO) has established that an initial report to NCSC (now BACS) is due within 24 hours of detection, and a follow-up with a detailed report is due within 14 days.
Enforcement & penalties	Fines up to CHF 100,000 from October 2025
Entry into force and/or relevant timelines	The Information Security Act (ISG) entered into force on 1 January 2024, while the Cybersecurity Ordinance (CSO) took effect on 1 April 2025 – establishing a 6-month grace period until October 2025, when penalties take effect.

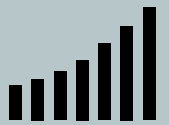
 UNITED KINGDOM	
Implementation status	● In progress
Transposing legislation	Cyber Security and Resilience (CS&R) Bill
Official link	/
Authority in charge	The National Cyber Security Centre (NCSC), under GCHQ, will provide guidance and technical policy; the Information Commissioner's Office (ICO) will oversee digital sectors; and sector regulators will have enforcement powers for critical infrastructure.
Deviations or additions	The UK version proposes a two-stage incident notification process (initial report within 24 hours, full report within 72 hours), along with obligations for board-level accountability, resilience testing, and supply chain risk oversight. Ransomware reporting may be mandated under additional legislation.
Enforcement & penalties	Fines up to £17 million or 4% of global turnover
Entry into force and/or relevant timelines	The UK is not transposing NIS2 but is developing its own Cyber Security and Resilience (CS&R) Bill, announced in the King's Speech in July 2024. A policy paper was published in April 2025 outlining key provisions. Draft legislation is expected to be introduced in late 2025 or early 2026. Legislation may be passed in late 2026, with enforcement to follow in 2027.



06

How Secomea supports you in achieving NIS2 compliance

Security, solutions, and features for your NIS2 readiness



Concrete examples of how can we help you in your NIS2 journey

The implementation of Secomea's Secure Remote Access solution aligns with the technical measures that you are required to take under Article 21 of the NIS2 Directive to manage the risks posed to the

security of network and information systems and prevent or minimize the impact of incidents.

Additionally, using Secomea will address the following elements mandated by the legislation.

NIS2 requires you to:

- **Implement access control policies and asset management:**

Managing and controlling access to your assets is precisely what Secomea is for.

With Secomea, you can

- ◇ provide access to defined assets
- ◇ handle role-based access permissions for each of your users and each of your devices
- ◇ provide access to users after they have requested it
- ◇ provide access to users for a defined timespan

- **Implement Multi-Factor Authentication:**

With Secomea, you can

- ◇ enable Multi-Factor Authentication using
 - o SMS Authentication
 - o Single-Sign-On (SSO)
 - Microsoft Entra ID (formerly known as Microsoft Azure Active Directory or Azure AD)
 - Okta



- **Have a plan in place to handle incidents and ensure business continuity (crisis management and disaster recovery):**

Secomea enables you to connect (and disconnect) machines to your network. This means that should a problem arise—e.g., a cyber-attack infecting one or more of your devices—you can use Secomea to cut that machine's access to your network, thereby preventing viruses or malware from spreading to other machines.

Therefore, Secomea is an essential tool for handling incidents and a crucial component in your organization's business continuity, crisis management, and disaster recovery plan.

With Secomea, you can

- ◇ review **audit logs** and **session recordings**. Should an incident occur during a remote access session, you'll be able to check who accessed the affected asset, when, for how long, and what they did. This will help you identify the cause of the incident and mitigate it.
- ◇ set-up up **alerts, events**, SMS/email alarms, and **automated actions** to get notifications of specific events related to your machines' status
- ◇ prevent risks when downloading files on your machines by using the **secure file transfer** feature; the feature ensures all files transferred to and from an engineering station are scanned for viruses or malware before they are accessible to the user.
- ◇ access the **Vulnerability Hub** to assess your overall vulnerability score based on the risks you run due to outdated firmware on gateways and identify the necessary actions to prevent downtime. For each gateway in every one of your sites, get notified if you need to update its firmware to the latest version or replace hardware that has reached End of Support.

NIS2 requirement	Secomea's features that help you address it
Access control policies and asset management	• Network management and customization to your company's internal policies • Appliances access management • User access management • User and asset control • Request for access
Multi-Factor Authentication	• 2FA & MFA – SMS Authentication – Single-Sign-On (SSO) ◊ Microsoft Entra ID (formerly Azure Active Directory, AD) ◊ Okta
Incident handling and business continuity	• Audit logs • Alerts, events, SMS/email alarms, and automated actions • Data Collection Module • Secure file transfer • Vulnerability Hub



NIS2 requires you to assess and ensure supply chain security – and Secomea can support you in doing that

Secomea's role in aiding you with supplier risk assessment is twofold:

» As a secure supplier:

As your secure remote access provider, Secomea is one of your suppliers whose risks and vulnerabilities you need to assess under the NIS2 Directive. We make that easy for you with our third party audit assessments:

- Our solution is certified under **IEC 62443-4-1 and compliant with IEC 62443-4-2 & IEC 62443-3-3** standards
- Our organizational security measures are based on **ISO 27002** and documented in an **ISAE 3402** report

Moreover, Secomea is an official CVE Numbering Authority (CNA), the first in Denmark.

» As a guarantee of security of the other suppliers you rely on who use Secomea:

Secomea is used worldwide by over 8,000 companies in the manufacturing and industrial machinery sectors.

Standardizing remote access for all stakeholders in this ecosystem is integral to our company mission.

As you evaluate the risks associated with your suppliers, you will likely find that many of them rely on Secomea as well.

This will give you assurance of the security of their remote access processes – and, in turn, **save you time when rating their risk level.**

The NIS2 Directive requires you to gather details regarding the security measures of every supplier and service provider you work with – a task that becomes increasingly challenging the more complex your OT setup is.

Secomea's Secure Remote Access (SRA) solution, purpose-built for industrial networks and OT equipment, has been empowering manufacturers and machine builders for over 15 years.

At Secomea, we've been engaging with customers and users since the onset of the NIS2 Directive to support them as they embark on their compliance journey.

Below is a selection of resources to help you get started with your NIS2 program.

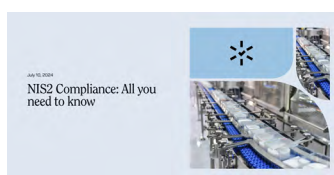


Learn more about Secomea's security

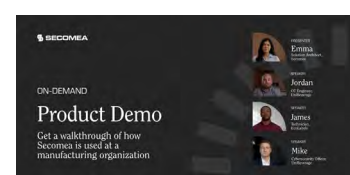
Expert insights and practical recommendations



[Download the whitepaper](#)



[Read the blog post](#)



[Watch demo on demand](#)

About Secomea

Offices in Denmark (HQ), US,
China, Japan

70+
Partners

+8,000
customers worldwide

+400,000
Gateways installed

CHR HANSEN

 Upfield™

 NOVARTIS

P&G

GEA

MQWI

TMEiC
We drive industry

MacArtney
UNDERWATER TECHNOLOGY

YASKAWA

 Weil
Technology

