Luxgap

DATA PRIVACY PARTNER

# NIS2 - The missing link for your business!

By Julien Winkin

# Introduction – Why this conference ?
# conference ?

1 **Problem**

The majority of the **new** companies concerned are still unaware of their obligations under NIS2.

2 **Objectives**

- **Identify the companies affected and their specific obligations**.
- **Present concrete actions and tools** to ensure compliance.
- **Clarify the exemptions for SMEs and the specific obligations for large companies**.

> NIS2, a constraint or an opportunity to strengthen the cybersecurity and resilience of your organisation?

# Our Expertise – who we are

Luxgap

DATA PRIVACY PARTNER

1 **External CISO & DPO services**

We act as external Chief Information Security Officers (CISO) and Data Protection Officers (DPO), ensuring your business is secure and compliant.

2 **Data protection & privacy compliance**

We assist companies in aligning with national and international regulations, including GDPR, AI Act, and other industry-specific laws.

3 **AI Compliance & governance**

Helping businesses integrate AI solutions while maintaining compliance with evolving regulations.

4 **Security & risk management**

We provide robust governance frameworks, risk assessments, and security audits to mitigate threats.

5 **Continuous training & support**

Employees are trained through our e-learning platform to ensure compliance at all levels.

IMMOTOP.LU
AG2R LA MONDIALE
DELEN
PRIVATE BANK
LUXEMBOURG
planning familial
COSTANTINI
CHdN
CENTRE HOSPITALIER DU NORD
Dussmann
FEDAS
LUXEMBOURG
CMCM
ÄR GESONDHEETSMUTUELLE
ZANTER 1956
LISER
LUXEMBOURG INSTITUTE OF SOCIO-ECONOMIC RESEARCH
ACL
co·labor
Zesumme fir de Mënsch a fir d'Natur
sympass

# Who is affected by NIS2?

## Expansion of the scope

**Sectors and organization** :

- **Highly critical (Annex I)**: energy, transport, banking, financial market infrastructures, health, water, digital infrastructure, ICT service management, public administration, space.
- **Critical (Annex II)**: postal services, waste management, food production, manufacturing, digital providers, research.

## Classification of entities

**Essential entities**:

- Large **enterprises** (250+ employees / €50M turnover or €43M balance sheet) **in the highly critical sectors**.

**Important entities**:

- Medium **enterprises** (50-249 employees / €10-50M turnover or €10-43M balance sheet) **in the critical sectors**.

## Exemption for SMEs

**Enterprises with less than 50 employees or less than €10M turnover are excluded**, except for:

- **Providers of electronic communications services**
- **Providers of cloud computing, DNS, domain name registration services**
- **Central public administrations**
- **Operators identified as critical at national level**

# Exceptions – entities subject to subject to NIS2 regardless of of size

The NIS2 Directive applies to entities listed in Annex I or II, regardless of their size, in the following cases:

⚠️ **Notice: This is an exception!**

Regardless of your company's size or revenue, you are required to comply with **NIS2**

# Entities Providing Critical Services

1. **Public electronic communications networks and services services**

2. **Trusted service providers**

   (e.g., electronic signatures, authentication services)

3. **Top-level domain name registries and providers of of domain name system (DNS) services**

⚠️ **Notice: This is an exception!**

# Other Entities Subject to NIS2

### Sole essential service provider in a member state

If an entity is the **only provider** of a service **essential** for maintaining critical societal or economic activities in a Member State, it is subject to NIS2 compliance.

### High-risk disruptions affecting public welfare

Entities must comply if a disruption of their services could:

- Have a significant impact on public safety, security, or health
- **Pose a systemic risk**, particularly in sectors where disruptions could have a cross-border impact

### National or regional critical entities

Entities are subject to NIS2 if they are classified as critical based on:

- Their national or regional importance to a specific sector
- Their role in interdependent sectors within a Member State

### Public administration entities

NIS2 applies to public administration organizations, including:

- Central government entities, as defined by national law
- Regional authorities providing essential services, where disruption could significantly impact societal or economic stability

**Key Takeaway:** Even SMEs and smaller organizations can fall under NIS2 obligations if they operate in critical sectors, are the sole provider of essential services, or play a major role in national or regional infrastructure.

# Does a 49-employee company selling financial software to banks need to comply with NIS2 ?

A **49-employee company selling financial software to banks** is **not automatically subject to NIS2**, **unless** it falls under one of the exceptions where size does not matter.

1️⃣ **If it only sells financial software to banks (without operating critical infrastructure or digital services)** → **Not subject to NIS2**, as it does not meet the **50-employee / €10M turnover threshold**.

2️⃣ **If it provides essential digital services (e.g., cloud computing, payment processing, or cybersecurity solutions for banks)** → **Subject to NIS2 regardless of size** (as a digital service provider or critical infrastructure).

3️⃣ **If it is classified as a nationally critical entity** → It could still fall under NIS2 even if it has fewer than 50 employees. **But you will be notified !**

**Conclusion:**
➡️ **If this company only sells software to banks and has fewer than 50 employees or €10M in revenue, it is not subject to NIS2.**
➡️ **If it offers essential digital services or is identified as critical, it is subject to NIS2, regardless of its size.**

# Why are 80% of companies not ready?

## The 5 major flaws observed

### Lack of governance

No dedicated cybersecurity manager.

### Insufficient subcontractors security

Uncontrolled dependencies. Data breach

### Executive training deficit

Little or no training for executives, who are **personally responsible** under NIS2.

### Inadequate incident management

NIS2 requires notification **within 24 hours** in the event of a significant incident.

### Poor risk management

No asset mapping, no vulnerability assessment.

**Real case : a** company deliberately concealed a data breach until it became evident that the stolen data was being exploited by hackers. Only then, several months later, did it officially disclose the incident, while downplaying its true impact. Although the fine remains confidential, the reputational damage is severe and long-lasting.

**62% of cyberattacks target suppliers to reach larger companies.**

**54% of companies have experienced a data breach resulting from an attack on a first-tier subcontractor, and 38% due to an attack on a second-tier or lower subcontractor.**

| Regulation | Notification Deadlines |
|---|---|
| NIS2 (EU Directive 2022/2555) | 24h (early warning) + 72h (detailed notification) + 1 month (final report) |
| GDPR (EU Regulation 2016/679) | 72h after detection |
| AI Act (pending adoption) | Not yet precisely defined (likely 24-72h under discussion) |
| DORA (Digital Operational Resilience Act - finance sector) | Notification within 4h after detection |
| CER Directive (Critical Entities Resilience Directive - critical infrastructure) | To be defined by each EU member state (often aligned with NIS2) |
| PSD2 (Payment Services Directive - banking sector) | Immediate notification + full report within 24h |

# Governance & responsibility - Where to start?

**Appoint a Chief Information Security Officer (CISO) or equivalent & always inform the DPO !**

**Implement quarterly reporting**

Key indicators: number of incidents, response time, compliance.

**Train the management team**

**Mandatory under NIS2!**

Always involve the DPO, as they are **listened to and followed** by everyone, including top management. Their impact is always significant, and they are the **key person for compliance** within the company due to their authority, position, and access to all projects.

# Supply Chain Cybersecurity

**Mandatory cybersecurity clauses (Already done with GDPR !)**
In supplier contracts (ISO 27001, SOC 2).

**Annual audit of critical providers**
At a minimum, signed due diligence is required

**Implementation of an emergency plan**
To address a supplier vulnerability, to change supplier...

According to the ENISA report, **86%** of organizations have implemented a **supply chain cybersecurity policy**,
yet only **47%** have allocated a dedicated budget, and **76%** lack **specific roles** for managing supply chain security;
while **61%** require security certifications from suppliers, only **48%** have a structured **vulnerability management process**,
and **13.5%** have no visibility over more than **50%** of their assets' patching status,
highlighting significant gaps in cybersecurity governance and risk management.

# Incident response - The 24-hour rule

### Mandatory notification within 24 hours

To the competent authorities.

### Deployment of an Incident Response Plan (IRP)

Tested regularly.

### Simulated attacks and crisis exercises

(Red Team, Purple Team, Blue Team).

**Concrete example**: For example, a basic vulnerability scan shows that companies that have never performed one always have open security gaps, making them easy targets for hackers. This leaves them exposed to attacks without even knowing it.

# Tools to automate NIS2 compliance

Some categories of solutions

- **Threat detection and response**: **EDR/XDR, SIEM, SOC**.
- **Data protection**: encryption, **DLP (Data Loss Prevention)**.
- **Compliance & risk management tools**

**Concrete example**: A company invested in several security tools, but after a few years, we assessed their effectiveness and found that they were no longer being managed. As a result, their value had diminished completely.

Do not automate everything, keep control !

# Fines & Responsibilities

### Sanctions for non-compliance

- **Essential entities**: maximum fine of **€10M or 2% of annual turnover**.
- **Important entities**: maximum fine of **€7M or 1.4% of annual turnover**.
- **Executives can be personally sanctioned!**

### Control methods

- Regular audits and inspections.
- Requirement for documentation and reporting to authorities.

# Immediate action plan

1. Identify if your business is affected by NIS2.

2. Conduct a cybersecurity audit audit and map the risks.

3. Secure your subcontractors and and partners.

4. Implement an incident response plan and test it.

5. Automate controls and reporting with suitable tools.

**Join us at our booth for a relaxed conversation!**

Have questions about NIS2 and compliance?

**Stop by our stand, grab a drink, and let's discuss** how we can help your business navigate these new regulations.

We look forward to meeting you!

contact@luxgap.com

Luxgap

DATA PRIVACY PARTNER

LUXGAP.COM

Thx!