# NIS2 Directive

The NIS2 Directive aims to strengthen the cybersecurity framework across the European Union (EU) by expanding the scope, enhancing risk management, and introducing stricter supervisory and enforcement measures. The directive is set to become law on **17th October 2024** in all EU Member States. NIS2 builds upon the original NIS directive to address the evolving cybersecurity landscape and ensure greater resilience against cyber threats.

## The key changes you need to know

- **Expanded Scope:** NIS2 includes additional critical sectors such as public administration, space, waste management, and the manufacturing of certain critical products. It also now applies to medium and large enterprises in critical sectors, including 5G infrastructure.
- **Increased Penalties:** Introduces stricter enforcement mechanisms and higher penalties for non-compliance, with fines reaching up to €10 million or 2% of the entities' total worldwide turnover, whichever is higher.
- **Enhanced Risk Management:** Emphasises measures for handling security incidents, conducting risk assessments, and implementing security policies and procedures to mitigate risks.
- **Incident Reporting:** Requires entities to report significant incidents within 24 hours of detection and submit a final report within one month.
- **Supply Chain Security:** Obligates entities to address and manage cybersecurity risks within their supply chains.
- **Cooperation and Information Sharing:** Enhances cooperation and information sharing between member states.
- **Harmonisation and Standardisation:** Aims to harmonise cybersecurity measures and protocols across the EU to reduce fragmentation.

## How DPRM can help with NIS2 Compliance

- **Quantum Safe Data Protection:** Certes offers strong quantum-safe encryption to protect data wherever it travels ensuring data security across all stages of the data lifecycle.
- **Separation of Key Policy Ownership:** Ensures that the control of protection parameters remains with the customer or data collector, reducing risks associated with regulatory penalties.
- **Data Security Unified Reporting:** Offers real-time insights into data security and potential vulnerabilities, aiding in compliance with incident reporting requirements.
- **Supply Chain Security:** Certes helps manage and mitigate risks in supply chains by providing end-to-end encryption and data protection solutions that extend to third-party vendors.

## What impact will NIS2 have on your organsation?

### Increase Compliance Costs

Implementing the required security measures and compliance activities will likely incur additional costs.

### Operational changes

Update operational processes, invest in new technologies, and enhance staff training to meet the new requirements.

### Increased resilience

Compliance efforts will lead to greater resilience against cyber threats, enhancing trust and confidence in digital services.

**Keep your data Secret,**
**Keep your data Certes**

**Certes.ai**
+1-412 262 2571
info@certes.ai