HYPERGENE
ENABLING BETTER PERFORMANCE

2025

# Hypergene Group White Paper NIS2 & DORA directive

APPROACH ON IMPLEMETING NIS2 AND DORA DIRECTIVE FOR HYPERGENE GROUP AND HYPERGENE PRODUCTS

# Content

# White Paper for NIS2 and DORA Directive

The scope of this White Paper encompasses the strategic initiatives and operational frameworks of the Hypergene Group, including its subsidiaries, Hypergene AB and Thinking Portfolio Oy. This document aims to provide a comprehensive overview of the directives and Hypergene Group's approach to comply with them.

# NIS 2[1] | Introduction

The NIS2 Directive aims to achieve a high common level of cybersecurity across the Union. Compared to NIS, clearer requirements are set for risk analyses and various security measures. Many other organizations will also be covered.

The purpose of the regulation is to increase cyber security within society, making us more resilient to cyber threats of different kinds.

NIS2 places clearer requirements on, among other things, risk analyses and various security measures. The directive also places increased demands on management participation in the organization's cybersecurity work.

NIS2 also means that significantly more sectors are covered by the legislation compared to NIS. For this reason, more supervisory authorities will be added. The penalty fees will also be higher than today in the event that the requirements are not complied with.

The NIS2-directive will be applicable primarily for currently 18 sectors that are identified as critical (for national defense), for example, energy, transportation, banking, finance, healthcare among others.[2]

The NIS2-directive will also be applicable for other organizations and businesses. The requirements are the same, however the reporting and sanctions are different.

In some extent, the NIS2-directive has a dependency to the CER-directive (Directive on the resilience of critical entities) requiring measures to increase resilience for critical activities.[3]

## The main content in NIS2

Providers of critical services must conduct systematic and risk-based information security management work supported by ISO27000-standard. Although the details are not published yet, there are a few main areas that are applicable:

### Establish and maintain a systematic approach to information security

The NIS2 Directive places requirements on, among other things, risk analyses and various security measures/risk management measures according to identified needs of the organization.

Additionally, there is a requirement for management education in risk analysis and security measures, as well as regular training in information security for employees.

### Report significant incidents

Organizations/ business must report all significant incidents to appointed authority in Sweden or Finland. This helps to create a comprehensive picture of the incident situation, warn others and initiate any coordinated efforts.

[1] Det här är NIS2-direktivet (2025-01-09)
[2] L_2022333SV.01008001.xml (2025-01-09)
[3] The Critical Entities Resilience Directive enters into application to ensure the protection of critical infrastructure in the EU - European Commission (2025-01-09)

# Timeline for implementation of NIS 2

## Sweden

The NIS2 Directive will be implemented in Sweden in the summer of 2025 at the earliest.

## Finland

The NIS2 Directive will be implemented in Finland in the spring of 2025 at the earliest.

## NIS2 applicability for Hypergene Group

Hypergene Group will probably not be included in the primary target group, since the organization is not included in the identified 18 sectors. However, Hypergene has customers that are within the appointed sectors and the requirements on them are assumed to be cascaded down to Hypergene and Hypergene's products.

# DORA[4] | Introduction

Digital Operational Resilience Act, (DORA) is an EU-directive with the purpose of strengthening the digital operative resilience for financial operations, by implementing a systematic approach in handling it-risks. The DORA directive is applicable within the financial industry i.e. banking, insurance companies, investment companies among others, that has the Financial Inspection Authority as supervisory authority. The directive is in force from January 2025.

## The main content in DORA

Companies within the financial sector are to comply with

- Handling risks within information and communication technology (ICT)
- Report incidents related to ICT
- Testing digital resilience
- Handling third party risks (ensuring suppliers of it-services comply with security measures required
- Information sharing (collaboration and share of information between companies to improve common security)

## DORA applicability for Hypergene Group

Hypergene will be applied to by the DORA directive indirectly by requirements on our IT services that are provided to financial customers.

[4] Förordning - 2022/2554 - EN - EUR-Lex (2025-01-09)

# Alignment | Hypergene's commitment to key indirect requirements

Hypergene Group has demonstrated its adherence to the following key controls, which are essential from the perspective of standards such as DORA and NIS2, through its ISO 27001 certification. These controls not only align with best practices in information security but also support its customers in meeting their own compliance obligations. By proactively implementing these measures, Hypergene strengthens operational resilience and maintains the trust of its customers.

## Vulnerability management

Hypergene takes an automated approach to vulnerability identification, ensuring that potential weaknesses in its systems are identified and addressed promptly. Regular vulnerability assessments and patch management processes are integral to safeguarding its services against evolving threats.

## Business continuity and testing

Hypergene's Business Continuity Plan (BCP) ensures operational resilience in the face of disruptions. Regular testing and scenario-based simulations validate the effectiveness of its continuity measures, enabling the company to provide uninterrupted service to its customers.

## Incident handling

A well-defined incident handling process allows us to respond quickly and effectively to security incidents. This includes monitoring, detection, containment, and recovery processes that minimize impact and ensure a swift return to normal operations.

## Backup and recovery

Hypergene implement comprehensive backup strategies across all critical systems to ensure data integrity and availability. Regularly tested recovery processes provide confidence that its data and services can be restored promptly in the event of a disruption.

## Multifactor authentication (MFA)

To enhance user security, Hypergene implements multifactor authentication (MFA) across its systems. The company's solution is designed to support the authentication methods chosen by its customers, allowing seamless integration with their preferred identity providers. This flexible approach ensures both robust security and an optimized user experience, tailored to individual business needs.

## Supporting Hypergene’s customers in meeting new directives

Hypergene understands that the evolving requirements of directives like DORA and NIS may introduce new obligations for its customers and their suppliers. As a trusted partner, the company is committed to providing the necessary support to help its customers meet these demands. Hypergene's team is readily available to answer questions, share insights, and collaborate on solutions that ensure compliance and operational resilience. Additionally, the company is happy to conduct joint exercises and simulations with its customers to practice and enhance their preparedness for regulatory requirements. Together, Hypergene and its customers address regulatory requirements efficiently and effectively.

# Conclusion | Hypergene Group compliance with NIS2 and DORA

Hypergene Group has implemented a management system for information security according to international standard ISO27001. The Management System for Information security includes a systematic approach concerning risk management and security measures.

Hypergene has a structured process for education and training with a focus on information security.  The main purpose of training is to strengthen the overall resilience in the organization towards information security threats.

Considering that Hypergene has a certificate for information security ISO27001 in place, the organization will most likely comply with both directives NIS2 and DORA. The expectation is that minor changes will be needed when the detailed content in NIS2 is finalized.

It is also expected that Hypergene's customers will have requirements for both organization and products/services based on NIS2 directive and DORA-directive.

Hypergene is monitoring status for the NIS2 directive and DORA-directive in both Sweden and Finland and will act when notified of upcoming changes.

//

Stockholm 2025-02-06

Jakob Melander, Chief Technology Officer (CTO)

Erik Thelander, Chief Product Officer (CPO)