ADDSECURE

New EU directive
with effect from October, 2024

NIS2 guide

Ensuring cyber security and readiness for your organisation

Checklist & recommendations

For a safer and smarter world

ADDSECURE

Introduction

The new EU directive NIS2 is here to ensure stronger cyber security resilience in vital functions on which we all depend, as individuals, society and corporations.

Expected to be in effect 2025, thousands of organisations and suppliers across the EU have the chance to level up their cyber security capabilities and demonstrate their commitment to protecting critical infrastructure.

However, becoming NIS2 ready can be a stressful challenge. NIS2 involves many more organisations and companies than the previous NIS and it can take an effort to become compliant. By many customers and business relations we are told that there is still confusion and a steep learning curve ahead.

This guide aims to help clairify the implications of NIS2 and offer some hands-on recommendations.

Don’t wait to get started

Whether your organisation is NIS2 ready by October 2024 or if you struggle to catch-up in the following year, it means not only having your cyber defenses under control, but also includes obligations regarding your supply chain and suppliers.

NIS2 is less voluntary than NIS, in terms of enforcement and sanctions. There are likely learnings from the implementation of GDPR in 2018, suggesting that many organisations certainly will not be ready from day one, but that national supervisory authorities initially will be hesitant to pursue legal actions.

But keep in mind: the legal responsibility is 100% on the management of your organisation. NIS2 is of critical importance for society as a whole, and compliance is mandatory.

Managers in an organisation, not only IT officers, can be held accountable in the event of incidents, with potential fines or sanctions being significant.

We respect that this can be complex and demanding, but we can help provide solutions for many of your needs.

Let’s collaborate to protect our organisations and countries. By setting requirements, conducting thorough checks, and supporting one another, we can create secure environments together.

One of the biggest challenges of NIS2 is being legally responsible also for the readiness of **all your third-party suppliers throughout the supply chain**: just trusting their assurance of being on top of their cyber security won’t do any more.

Krister Tånneryd
Chief Operating Officer,
AddSecure Group

What is NIS2?

A new EU directive, to better protect society's critical infrastructure

The objective of NIS2 is to protect critical entities in society by applying stricter cyber security standards, protecting data and the supply chains of infrastructure. Rapid incident reporting and strengthening cooperation among EU members on cyber security is also important.

Cyber threats and ransomware must be countered
The need to protect vital societal infrastructure from cyber threats has increased rapidly in recent years. Hackers continue to evolve and innovate, with AI tools having the potential to make cyber criminals create even more sophisticated threats and ransomware. State-sponsored hacking, cyber espionage, and cyber warfare add to the complications.

In 2016, the first NIS Directive (Network and Information Security Directive) was adopted by the European Union to increase the overall level of cyber security within the EU and improve the resilience of critical infrastructure.

Introduced in 2022, the new NIS2 Directive responds to the on-going rise and development of cyber threats, and is set to be in effect by national legislations in October 2024. (In some countries the implementation may be delayed until early 2025).

WARNING

Public services and supply chains are especially attractive targets for hackers, as any service disruption can have dangerous consequences and demand immediate rectification.

About NIS2

NIS2 is a new European Union directive aimed at improving the cyber security posture of member states. Building on the original NIS Directive of 2016, NIS2 sets higher standards for cyber security, risk management, and reporting across various sectors to enhance the overall resilience of critical infrastructure.

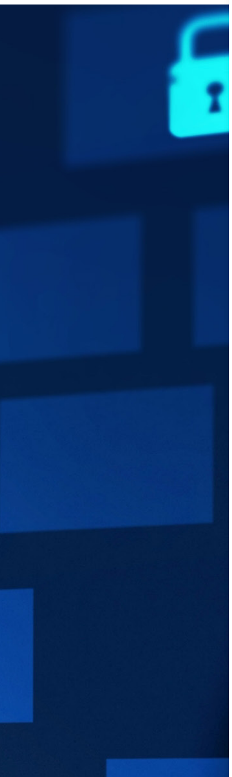
Which organisations does NIS2 apply to?

NIS2 applies to more organisations than the previous NIS. It focuses on entities essential for critical infrastructure, divided into two categories: **’essential’** and **’important’**. Disruptions in the essential group would have serious societal consequences for a country, while disruptions in important entities, often medium-sized, may not have severe social or economic consequences but significantly impact supply chain resilience.

Does NIS2 apply to all companies and organisations in the EU?
No. NIS2 covers specific essential and important sectors and their activities, excluding very small companies in these sectors, with some exceptions.

Which sectors are now covered by NIS2?
Below is a list of entities covered by the NIS2 directive.

One of the important changes in NIS2 is that from now on public administration and municipalities will be included, as ’essential’ entities.



Essential entities

Threshold
> 250 employees
> €50 million turnover
> €43 million balance

ESSENTIAL

- Energy (electricity, district heating, oil, gas, hydrogen)
- Transport (air, rail, water, road)
- Banking
- Financial market infrastructure
- Health (hospitals, EU reference laboratories, research and development of medicines)
- Drinking water
- Waste water
- Digital infrastructure (IXP, DNS service providers, TLD name registries, cloud computing services, data center services, content delivery networks, electronic communications, trust service providers)
- Public administration (state, regional, and local authorities)

Important entities

Threshold
50 - 249 employees
€10 - €50 million turnover
€10 - €43 million balance

IMPORTANT

- Postal and courier services
- Waste management
- Chemicals (manufacturing, production, distribution)
- Food (production, processing, distribution)
- Manufacturing (medical devices, computers, electronic and optical products, electrical equipment, machinery, motor vehicles and trailers, transport equipment)
- Digital service providers (online search engines, online marketplaces, social networking services platforms)
- Space

Is your organisation among these?

Main objectives of NIS2

- **Implement asset management practices** to identify and protect critical information systems and assets.
- **Report to relevant authorities** and maintain incident response capabilities.
- **Formulate and put into action cyber security strategies** along with risk management protocols.
- **Establish protocols** for handling incidents, mandates for reporting, and response plans.
- Devise a strategy to **guarantee the consistent delivery of critical services** during cyber incidents.
- **Put into action supply chain security measures** to review and guarantee the safety of third-party providers.
- **Provide training and heighten awareness** among employees about optimal cyber security protocols.
- **Ensure incidents are reported** to the appropriate bodies and uphold the capability to respond to incidents.
- **Eliminate inconsistencies** and improve communication and cooperation between member states.

What NIS2 means for your organisation

NIS2 brings new demands for many companies or organisations regarding cyber security. Some can be handled by an IT department, some concern responsibilities at a management level, and others require the involvement of all employees.

It’s not a one time quick-fix but something that will demand ongoing attention and resources.

IT security is not just about technology and is no longer solely an issue for the IT department. It involves people, processes, and technology, and today, digital risks and threats are a matter for the management.

- **Enhanced security requirements**: Organisations will need to implement comprehensive risk management and cyber security practices. This includes incident prevention, detection, and response measures.
- **Supply chain security**: Organisations must ensure that all supply chain and service providers also meet the cyber security standards of NIS2.
- **Management accountability**: Senior management will be held accountable for compliance, meaning they must ensure their organisation meets all the directive’s requirements.
- **Broader scope**: More sectors are covered under NIS2, including healthcare, digital infrastructure, and public administration. Even small and medium-sized enterprises in these sectors may need to comply.
- **Incident reporting**: There are stricter obligations for rapidly reporting cyber security incidents. Organisations must implement procedures for rapid and accurate reporting of significant cyber security incidents to relevant authorities.

Documentation under NIS2

Under NIS2, organisations must have formal policy documents and maintain documentation of their cyber security measures, and logs of incidents, which are regularly reviewed and can be presented to authorities upon request.

Failure to demonstrate this documentation would mean non-compliance with NIS2 requirements.

Checklist: How to preprare for NIS2

Timely preparation is key to becoming fully NIS2 ready.

1. **Understand the requirements**
Familiarise yourself with the NIS2 directive and its implications.
Example: Check if your company falls under essential or important categories.

2. **Create a cyber security policy document**
Develop and maintain a comprehensive cyber security policy document.
Example: Include sections on risk management, incident response, and supply chain security. Assign roles and responsibilities.
Tools: Follow templates and frameworks from standards like ISO 27001.

3. **Conduct a risk assessment**
Identify and prioritise potential cyber security threats.
Example: Look for risks like data breaches and ransomware.
Tools: Use risk assessment software and frameworks like ISO 27005.

4. **Implement security measure**
Create and enforce strong cyber security policies.
Example: Use multi-factor authentication and encryption.
Tools: Follow ISO 27001 and use firewalls, IDPS, and endpoint protection.

5. **Ensure supply chain compliance**
Make sure your suppliers follow your cyber security standards.
Example: Regularly audit your suppliers. Ask suppliers about their cyber security practices: Make them show proof like ISO 27001 certification.

6. **Set up rapid incident reporting**
Create clear steps for reporting cyber security incidents to designated authorities.
Example: Define what counts as an incident and how to report it.
Assign roles and set timelines for reporting. Practice with regular drills.

7. **Train your team**
Make sure that employees and management understand their roles in maintaining cyber security. Provide basic and advanced training for everyone. Regularly train them on security measures.
Example: Run phishing simulations and cyber security workshops.
Tools: Use interactive modules and real-world case studies.

8. **Monitor and review**
Continuously assess and improve your cyber security measures to stay compliant.
Example: Regularly conduct security audits and penetration tests.

By following these steps, you can prepare for NIS2 readiness, boost your cyber security, and stay protected against cyber threats.

Consequences of non-compliance

THE NIS2 DIRECTIVE INCLUDES STRICTER SUPERVISORY MEASURES

> Companys and organisations that do not comply risk fines of up to **€10 million** or **2% of total global turnover** for essential entities, and less for public authorities an smaller entities. Additionally, governing bodies or other senior positions may be held **personally liable** for violations. NIS2 shifts the responsibility for implementing and upholding cyber security measures from the IT department and now includes top management personnel.

Supervison: Each member state will have one or more designated competent authority responsible for ensuring compliance with the NIS2 directive. These authorities are tasked with overseeing the implementation and enforcement of the directive within their jurisdiction. They can e.g. perform on site inspections, regular audits (for 'essential' entities), or request full documentation of an organisation's or company's cyber security policy and implementation of safety measures.

Recommendation:
Ensure your third-party suppliers are ISO 27001 certified to simplify NIS2 readiness

Under NIS2, organisations are legally responsible for the cyber security of their entire supply chain, including third-party suppliers. This means you must actively verify and monitor suppliers at all times, not just rely on a one-off promise or written statement/contracts.

Tracking supplier compliance can be very challenging. One solution is to use specialist services that monitor suppliers. However, a more practical approach is to choose third-party solutions with relevant cyber security certifications like ISO 27001.

ISO 27001 is a global framework for information security management systems that aligns well with NIS2 requirements. Adopting ISO 27001 helps build a strong cyber security foundation and simplifies NIS2 readiness. ISO 27005 complements this by providing guidelines for information security risk management.

To ease NIS2 readiness, consider getting ISO 27001 certified or ensure all your third-party suppliers are ISO 27001 certified.

CERTIFIED ISO 27001 NORDIC CERTIFICATION

NIS2 and ISO 27001

NIS2 sets the framework for what your organisation needs to do, while ISO 27001 provides the tools and processes needed to meet the requirements. It includes standards for policy, processes, risk management and self controls.

How AddSecure can help

For many of our customers, NIS2 will bring significant changes. Companies and public authorities will need to allocate more resources to enhance their resilience against cyber criminals. We have substantial work ahead to collectively elevate the maturity of information security. At AddSecure, we are well-prepared and eager to assist our customers, suppliers, and partners.

It's gratifying that the EU is addressing this issue with the implementation of NIS2 and other forthcoming directives to make Europe safer. One can compare the impact of NIS2 on information security to the impact of GDPR on privacy.

ISO 27001 certified

AddSecure is an ISO certified provider, offering solutions and products that seamlessly integrate into your supply chain while ensuring compliance with NIS2 regulations.

Securing IT, OT, and all connected devices

Cyber security extends beyond IT (Information Technology), which covers everything within your organisation's firewalls, to also include OT (Operational Technology). OT involves the control and monitoring of processes and physical devices, often located outside your organisation. This includes connected sensors that transmit crucial data within supply chains for logistics or infrastructure. It's essential to ensure that IT, OT, and all connected devices adhere to cyber security regulations and remain under your control.

Connect your devices using AddSecure's secure IoT platform

AddSecure's secure IoT platform ensures reliable and encrypted communication between connected devices. ISO 27001 certified, it offers robust data transmission, continuous monitoring, and real-time incident management, enhancing the security and efficiency of IoT networks across various industries. By integrating this IoT solution, organisations can secure their supply chains and meet NIS2 requirements. The platform facilitates the creation of a private network (VPN) that isolates all devices and systems from other internet traffic and unauthorized access.

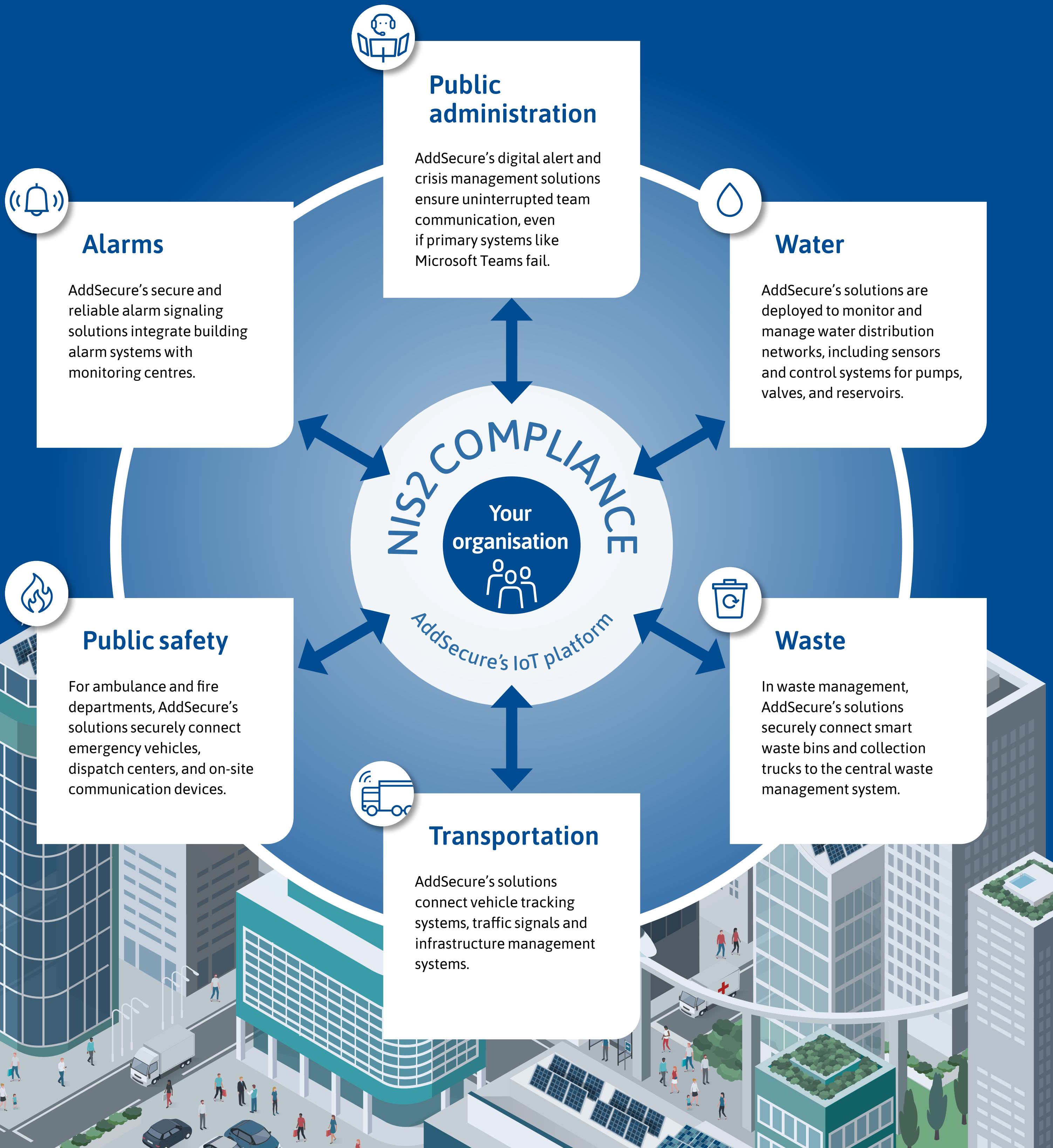
Secure back-up for internal communication during crises

Many organisations, particularly in public administration, rely heavily on applications like Microsoft Teams for video calls and digital meetings. To achieve NIS2 readiness, having a secure backup system for internal communications is crucial. AddSecure provides innovative digital solutions that ensure efficient and reliable communication during crises and emergencies.

NIS2 readiness with AddSecure

Today's society is full of connected devices and sensors transmitting real-time data and information, running logistics and distributing resources of critical importance. AddSecure provides solutions for secure communications, and with the AddSecure IoT platform, we ensure reliable and encrypted communication between all your connected devices.

Below are some examples of how AddSecure can help protect society's critical infrastructure.



NIS2 COMPLIANCE

Your organisation

AddSecure's IoT platform

Public administration

AddSecure's digital alert and crisis management solutions ensure uninterrupted team communication, even if primary systems like Microsoft Teams fail.

Alarms

AddSecure's secure and reliable alarm signaling solutions integrate building alarm systems with monitoring centres.

Water

AddSecure's solutions are deployed to monitor and manage water distribution networks, including sensors and control systems for pumps, valves, and reservoirs.

Public safety

For ambulance and fire departments, AddSecure's solutions securely connect emergency vehicles, dispatch centers, and on-site communication devices.

Waste

In waste management, AddSecure's solutions securely connect smart waste bins and collection trucks to the central waste management system.

Transportation

AddSecure's solutions connect vehicle tracking systems, traffic signals and infrastructure management systems.

Examples of how AddSecure contribute to secure supply chains and companies

Our IoT platform and communications solutions ensure NIS2 readiness, providing efficient and reliable communication during crises and emergencies across multiple sectors.

Alarms

Example: AddSecure's secure and reliable alarm signaling solutions integrate building alarm systems with monitoring centres.

- Application: When an alarm is triggered (e.g., fire, intrusion), the data is immediately sent to the alarm monitoring centre, which can then dispatch emergency services.
- Benefit: Provides reliable and secure communications to ensure quick response times and maintains the integrity and confidentiality of alarm data.

Public adminstration and municpalities

Example: During a major emergency, a municipal government can rely on AddSecure's alert and crisis management solutions, which support secure telephone and video conferencing, to ensure uninterrupted team communication, even if primary systems like Microsoft Teams fail.

- Application: By integrating AddSecure's digital alert and crisis management solutions, organisations can seamlessly switch to reliable telephone and video conferencing, ensuring uninterrupted internal communications during critical times.
- Benefit: This guarantees that essential communication channels are always operational, thereby enhancing the organisation's ability to respond effectively to crises and maintain operational continuity.

Public safety

Example: For ambulance and fire departments, AddSecure's solutions securely connect emergency vehicles, dispatch centers, and on-site communication devices.

- Application: Ambulances and fire trucks send real-time updates on their status, location, and incident details back to the dispatch center. On-site personnel can also use connected devices to share critical information.
- Benefit: Ensures efficient coordination and response during emergencies, maintains secure and uninterrupted communication, and protects sensitive information about incidents and patients.

Transportation

Example: In the transport sector, AddSecure connects vehicle tracking systems, traffic signals, and infrastructure management systems.

AddSecure

CERTIFIED ISO 27001 NORDIC CERTIFICATION

CERTIFIED ISO 9001 NORDIC CERTIFICATION

CERTIFIED ISO 14001 NORDIC CERTIFICATION

- Application: Real-time data from vehicles (e.g., location, speed, and engine health) is transmitted to the transport management center to optimise routes and manage traffic flow.
- Benefit: Enhances operational efficiency, reduces congestion, and ensures the security of data exchanged between moving vehicles and stationary infrastructure.

Water supply

Example: AddSecure's solutions are deployed to monitor and manage water distribution networks, including sensors and control systems for pumps, valves, and reservoirs.

- Application: Sensors detect leaks or changes in water pressure and report this data in real-time to the central water management system.
- Benefit: Ensures prompt response to issues, maintains consistent water quality and supply, and secures communication channels to prevent tampering or unauthorised access.

Waste management

Example: In waste management, AddSecure's solutions securely connect smart waste bins and collection trucks to the central waste management system.

- Application: Smart bins equipped with sensors can notify the central system when they are full. Collection schedules are then optimised and communicated to the trucks.
- Benefit: This ensures efficient waste collection, reduces costs, and prevents overflows, while maintaining secure data transmission and system integrity.

In all these sectors, AddSecure's IoT platform ensures that the communications between IoT devices and central management systems is encrypted and secure, preventing unauthorized access and ensuring the integrity and availability of critical data.

> NIS2 will bring significant changes, requiring more resources to enhance resilience against cyber criminals. At AddSecure, we are well-prepared to assist our customers, suppliers, and partners.

Mats Genberg
Chief Revenue Officer,
AddSecure Group

ADDSECURE

For a safer and smarter world

www.addsecuregroup.com