WHITE PAPER

NIS2 Enforcement: Fines and Warnings

COPIA

The EU’s Network and Information Security Directive (NIS2), effective from January 16, 2023, aims to enhance cybersecurity across critical sectors within the EU. NIS2 significantly broadens the scope of the original NIS directive, encompassing more sectors and organizations deemed vital to the EU economy and society. A key aspect of NIS2 is its enforcement mechanism, which includes substantial fines for non-compliance. While the specific implementation and penalties vary across member states, the directive sets a framework for significant financial consequences. This article explores the fines or warnings under NIS2.

> A key aspect of NIS2 is its enforcement mechanism, which includes substantial fines for non-compliance.

Understanding NIS2 and its Scope

With the increasing reliance on digital infrastructure and the rise in sophisticated cyberattacks, NIS2 seeks to establish a higher level of cybersecurity across the EU. It mandates that organizations in critical sectors implement appropriate security measures and report incidents with significant impact to the relevant authorities. The directive distinguishes between “essential” and “important” entities, with varying levels of fines for each category.

To determine if an organization falls under the scope of NIS2, one of the key factors is whether it **qualifies as a “large enterprise.”** This classification is based on criteria defined in Article 2 of the Annex to Recommendation 2003/361/EC, which considers factors like the number of employees and annual turnover.

Essential entities include those operating in sectors like:

- Energy
- Transport
- Banking and financial market infrastructure
- Healthcare
- Drinking water
- Public administration
- ICT services
- Digital infrastructure

Important entities include those in sectors like:

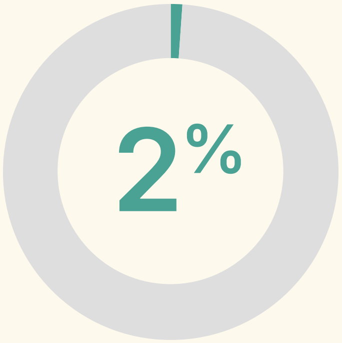
- Postal and courier services
- Waste management (only if it is an essential part of their general activity)
- Chemical manufacturing
- Food production and processing
- Manufacturing (machinery, equipment, transportation, etc.)
- Digital providers (online marketplaces, search engines, social networking platforms, etc.)
- Research institutions

In addition to these size-based criteria, some entities automatically fall under NIS2 regardless of their size due to their potential impact on essential services and public safety. These include:

- Providers of public electronic communications networks or services
- Providers of trust services
- Registries for top-level domain names and providers of domain name system (DNS) services
- Public institutions

Fines Under NIS2

NIS2 empowers member states to impose administrative fines for violations. These fines can be substantial, reaching up to €10 million or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher. The directive emphasizes a graduated approach to penalties, with higher fines for essential entities compared to important entities.



€10 million or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher

ENTITY TYPE	MAXIMUM FINE
Essential Entities	€10,000,000 or 2% of global annual revenue, whichever is higher
Important Entities	€7,000,000 or 1.4% of global annual revenue, whichever is higher

Despite these potential penalties, specific instances of companies fined under NIS2 are not readily available in public sources as of January 2025. This could be attributed to several factors:

- **Recent Implementation:** NIS2 was enacted in January 2023, with an initial deadline for transposition into national law by October 17, 2024. However, many member states missed this deadline, and are still in the process of transposing the directive. This suggests that enforcement actions, including fines, may still be in their early stages.
- **Confidentiality:** Information about specific fines might be kept confidential due to ongoing investigations, settlements, or data protection regulations.
- **Reporting Delays:** There could be a delay in publicly releasing information about fines due to administrative processes or reporting procedures.

Furthermore, the lack of publicly available information on fines could indicate a strategic focus on initial warnings and encouraging voluntary compliance before resorting to financial penalties. This approach allows organizations time to adapt to the new requirements and implement necessary cybersecurity measures.

Warnings Under NIS2

Similar to fines, concrete examples of companies warned under NIS2 are scarce in publicly accessible information. However, there are indications that warnings and notices are being issued. For example, the European Commission initiated infringement procedures against 23 member states for failing to implement NIS2 by the October 2024 deadline. These procedures serve as a formal warning to member states to comply with the directive.

A recent study by cybersecurity firm Sailpoint suggests that many organizations, particularly in the UK, are not fully prepared for NIS2 compliance. This lack of preparedness could lead to supervisory authorities issuing warnings to organizations lagging in their compliance efforts. For instance, organizations might receive warnings for failing to adequately secure their supply chains, assess the efficiency of existing cyber measures, implement necessary risk management measures, or provide cybersecurity training to staff.

Copia and NIS2 Compliance

Copia, as a Git-based version control and backup system for industrial automation, can help organizations in several ways to meet specific aspects of the NIS2 directive, particularly in areas related to:

1. **Risk Management:**
   - **Security in the acquisition, development, and maintenance of network and information systems (one of the 10 minimum security measures):** Copia's core function is managing the development and changes to automation code. By using a Git-based system, organizations can track every change, who made it, when it was made, and why. This detailed audit trail helps in identifying potential vulnerabilities introduced during development or maintenance and provides accountability.

> By using a Git-based system, organizations can track every change, who made it, when it was made, and why

- **Incident handling (one of the 10 minimum security measures):** While Copia doesn't directly handle incident response, it can play a vital role in recovery. If an incident involves compromised or corrupted automation code, Copia provides you the information to quickly revert to a previous known-good state, minimizing downtime and facilitating a faster recovery.
- **Vulnerability Handling and Disclosure:** Although Copia doesn't scan for vulnerabilities itself, the detailed version history it provides helps in tracing the origin of a vulnerability if one is found. Knowing exactly which code change introduced a weakness allows for faster remediation, aligning with best practices as laid out in the PLC Top 20 Secure Coding Practices.

2 Business Continuity:

- **Business continuity management (one of the 10 minimum security measures):** Copia helps ensure business continuity by providing a robust and reliable backup and recovery mechanism for automation code. Your PLC and other automation code is not just backed up; it's managed with full version history. This ensures that you can restore operations quickly after a cyber incident or hardware failure.
- **Disaster Recovery:** Copia's Git-based system enables automated backup and retention of automation code for accessibility during disaster recovery scenarios. Since the entire project history is stored off-site, you can restore your automation systems to their pre-incident state at any backed-up point in time.

3. **Security procedures for employees with access to sensitive data, including data access policies and asset management (one of the 10 minimum security measures):**

    - Copia can help with the management of your automation systems through access control. Copia supports minimum necessary access and least privilege access to your automation code and supports preventing unauthorized or accidental changes.
    - Copia is a central repository for your automation assets. You can think of it like a “single source of truth” for your automation code.

Specific Copia features that contribute to NIS2 compliance:

- **Version Control:** Tracks all changes to automation code, providing a detailed history that is crucial for audits, incident investigation, and understanding the evolution of your systems.
- **Rollback Capabilities:** Enables quick restoration to previous versions of code, storing it securely so that it can be rolled back to PLCs based on internal change management procedures. Having these files backed up and stored securely minimizes downtime during incident response and recovery.
- **Branching and Merging:** Facilitates secure development practices by allowing engineers to work on new features or fixes in isolation and then merge them into the main codebase after thorough testing and review.
- **User Access Control and Permissions:** Helps to establish roles and access rights, so only authorized individuals can make changes to the automation code.

Having these files backed up and stored securely minimizes downtime during incident response and recovery.

- **Centralized Repository:** Provides a single, secure location for storing all automation code, improving organization, accessibility, and security.
- **Change Management:** Copia's visual diffs allow you to compare versions of code quickly, so you can always see what's changed.

Limitations:

It is important to understand that Copia is a tool that aids in achieving NIS2 compliance but is not a complete solution for compliance with NIS2 in itself. It primarily addresses aspects related to automation code management. To fully meet NIS2 requirements, you will need a comprehensive cybersecurity strategy that includes other tools and processes for areas like:

- Network security
- Endpoint protection
- Intrusion detection and prevention
- Security Monitoring
- Strong encryption
- Supply chain security assessments
- Incident response planning and execution
- Employee security awareness training

In summary, Copia can be a valuable asset in your NIS2 compliance toolkit, especially for organizations heavily reliant on industrial automation. It strengthens your ability to manage risks, ensure business continuity, and contribute to secure development practices within your automation systems. However, remember to integrate Copia into a broader cybersecurity strategy to achieve full NIS2 compliance.

Key Requirements of NIS2

The NIS2 Directive outlines four overarching areas of requirements:

1. **Risk Management:** Organizations must adopt robust cybersecurity risk management practices, including incident handling, supply chain security, network and information system security, access control, and cryptography.
2. **Corporate Accountability:** Management bodies are now directly responsible for overseeing and approving cybersecurity measures. They are also required to undergo training and can be held liable for non-compliance, facing potential penalties such as temporary bans from managerial roles.
3. **Reporting Obligations:** Entities must establish processes for timely reporting of significant incidents. This includes an "early warning" notification within 24 hours of becoming aware of an incident, followed by a more detailed report within 72 hours and a final report within one month.
4. **Business Continuity:** Organizations are required to develop and implement business continuity plans to ensure the continued operation of essential services during and after major cyber incidents. This includes system recovery strategies, emergency procedures, and the formation of a dedicated crisis response team.

10 Minimum Security Measures

In addition to the four key areas, NIS2 mandates the implementation of 10 minimum baseline security measures:

1. Risk assessments and information system security policies.
2. Policies and procedures to evaluate the effectiveness of cybersecurity risk-management measures.
3. Policies and procedures regarding the use of cryptography and, where appropriate, encryption.
4. Incident handling plan.
5. Security in the acquisition, development, and maintenance of network and information systems, including vulnerability handling and disclosure.
6. Cybersecurity training and basic cyber hygiene practices.
7. Security procedures for employees with access to sensitive data, including data access policies and asset management.
8. Business continuity management plan, including backup management and disaster recovery.
9. 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.
10. Security of supply chains, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

Path to Compliance

Achieving NIS2 compliance requires a proactive and systematic approach. Organizations should consider the following steps:

1. **Determine Applicability:** Identify whether your organization falls under the scope of NIS2 and which specific units or departments are affected.
2. **Risk Assessment:** Conduct a thorough assessment of your current cybersecurity posture against the requirements of NIS2 to identify gaps and areas for improvement.
3. **Remediation Plan:** Develop a comprehensive plan to address identified gaps, including implementing new security measures, updating policies and procedures, and providing necessary training.
4. **Incident Response:** Establish or refine incident reporting procedures to comply with NIS2's strict notification deadlines.
5. **Continuous Monitoring:** Implement ongoing monitoring and auditing processes to ensure the continued effectiveness of security measures and maintain compliance.
6. **Supply Chain Security:** Engage with your suppliers to assess their cybersecurity practices and incorporate NIS2 requirements into contractual agreements.

Achieving NIS2 compliance requires a proactive and systematic approach.

Conclusion

The NIS2 Directive represents a significant step forward in strengthening cybersecurity across the EU. By taking proactive steps now, organizations can not only ensure compliance but also enhance their overall resilience against evolving cyber threats. The time to act is now, as the transposition deadline has passed and the typical compliance process can take 12 months to complete. Implementing robust cybersecurity measures is not just a regulatory obligation but a crucial investment in safeguarding critical infrastructure and maintaining public trust.

Take the Next Step in Your Journey

Concerned about the impact of NIS2 fines on your industrial operations? Copia simplifies a critical piece of the puzzle: securing your industrial automation code. Request a demo today to see how Copia integrates into your broader cybersecurity strategy.

You can also reach out directly by emailing contact@copia.io.

NIS2 Compliance Checklist

This checklist provides a high-level overview of key actions required for NIS2 compliance. It should be used in conjunction with the full text of the NIS2 Directive and tailored to your organization's specific circumstances.

Phase 1: Assessment & Planning

□ Determine Applicability:

- Identify if your organization falls under NIS2 (Essential or Important entity).
- Determine which parts of your organization are affected.

□ Leadership & Governance:

- Assign responsibility for NIS2 compliance to a specific individual or team.
- Ensure management bodies understand their responsibilities and liabilities.
- Develop a cybersecurity training program for management.

□ Gap Analysis:

- Conduct a thorough assessment of current cybersecurity measures against NIS2 requirements.
- Identify gaps and areas for improvement in risk management, reporting, and business continuity.

□ Risk Assessment:

- Develop or update a comprehensive cybersecurity risk assessment process.
- Identify and prioritize cybersecurity risks based on their likelihood and potential impact.

□ Plan Development:

- Create a detailed NIS2 compliance plan with timelines and assigned responsibilities.
- Develop or update cybersecurity policies and procedures to align with NIS2.

Phase 2: Implementation

□ Risk Management Measures:

- Implement the 10 minimum baseline security measures (outlined in the whitepaper).
- Establish an incident handling plan and response process.
- Develop policies for vulnerability handling and disclosure.
- Implement access control measures and data protection policies.
- Implement cryptographic solutions, including encryption where appropriate.

□ Supply Chain Security:

- Assess the cybersecurity posture of direct suppliers.
- Incorporate NIS2 requirements into supplier contracts.

□ Business Continuity:

- Develop or update a business continuity plan for major cyber incidents.
- Establish backup and disaster recovery procedures.
- Form a crisis response team and define roles and responsibilities.

□ Reporting Obligations:

- Establish procedures for reporting significant incidents within the required timeframes (24-hour early warning, 72-hour detailed report, one-month final report).
- Designate a point of contact for communication with relevant authorities.

□ Training & Awareness:

- Provide cybersecurity training to all employees, including specific training for those with access to sensitive data.
- Conduct regular awareness campaigns to promote a culture of cybersecurity.

Phase 3: Monitoring & Improvement

□ Auditing & Assessment:

- Conduct regular internal audits to assess the effectiveness of security measures.
- Engage external auditors for independent verification of compliance.

□ Continuous Monitoring:

- Implement systems for ongoing monitoring of network and information systems.
- Regularly review and update risk assessments and security measures.

□ Incident Review:

- Conduct post-incident reviews to identify lessons learned and improve incident response procedures.