Data Sheet

KEEPER

Simplify NIS2 Identity Security Compliance With Next-Gen Privileged Access Management

Is Your Organisation Prepared For The NIS2 Directive?

The NIS2 Directive (Directive (EU) 2022/2555) goes into effect in October of 2024. The NIS2 Directive extends the scope of its predecessor, the Network and Information Systems Directive, to cover a broader range of sectors and types of organisations due to the increasing reliance on digital technologies and the rising number of cyber threats. The directive aims to enhance the security of network and information systems within the EU, ensuring a high common level of cybersecurity. By revising the directive, EU member states aim to better defend critical industry sectors against ransomware attacks, supply chain vulnerabilities and more.

NIS2 covers more industry sectors than the original directive, and the requirements apply not only to organisations and their direct employees, but also the subcontractors and service providers supporting them.

NIS Industries	Expanded NIS2 Industries	
• Banking • Digital Infrastructure • Digital Service Providers • Financial Market Infrastructure • Energy • Healthcare • Transportation • Water Supply	• Chemicals • Digital Providers (Online Marketplaces, Search Engines, Social Networking Platforms) • Food Producers, Processors and Distributors • Health (Critical Medical Devices, Pharma, R&D) • Postal and Courier Services	• Public Administration • Space • Wastewater • Manufacturing of Critical Products (Computers, Electronics, Medical Devices, Motor Vehicles) • Providers of Public Electronic Communications Networks or Services

Failure to Comply Could Be Costly and Dangerous

If an organisation fails to meet the compliance mandates set in the NIS2 Directive, it can face several consequences, which are designed to ensure that entities take their cybersecurity obligations seriously. The nature and severity of these consequences can vary depending on the specific national legislation of each EU member state, as member states are responsible for transposing EU directives into their national law. However, the NIS2 Directive provides a framework for these penalties, aiming for a harmonised approach across the EU. The potential consequences include:

- Monetary Fines
- Periodic Penalty Payments
- Orders To Take Specific Actions
- Public Notices and Reputation Damage
- Operational Restrictions
- Liability for Damages

The enforcement of these consequences is carried out by national authorities designated by each EU member state.

Eliminate the Pain of NIS2 Compliance with KeeperPAM

Organisations within the European Union can leverage Keeper's Next-Gen Privileged Access Management (PAM) solution to easily and cost-effectively achieve compliance with the NIS2 Directive. By offering granular Role-Based Access Controls (RBAC), Keeper enables IT admins to manage privileged account access throughout the organisation, ensuring that users have only the necessary permissions to perform their roles. Advanced reporting capabilities provide clear insights into privileged account activities, aiding in continuous monitoring and simplifying the auditing required for NIS2 compliance. Keeper also empowers organisations of all sizes to enforce cybersecurity best practices, including the use of strong, unique passwords and Multi-Factor Authentication (MFA). At the heart of Keeper's solution is its zero-knowledge encryption model, which ensures that sensitive data is protected by industry-leading security, making it an ideal choice for EU organisations aiming to meet the NIS2 standards while enhancing their overall cybersecurity posture.

Streamline NIS2 Compliance

Requirement	Solution
Paragraph 49: Cyber Hygiene Policies	**Establish strong cyber hygiene policies with password management and least privilege access.** Keeper's industry-leading Enterprise Password Manager creates, stores, and manages complex and unique passwords for every user. Role-Based Access Controls (RBAC) allow administrators to precisely manage user permissions, ensuring individuals have access only to the resources necessary for their job functions to ensure least privilege throughout the organisation.
Paragraph 54: Ransomware	**Defend data and systems against ransomware.** Keeper enforces the use of strong and unique passwords and MFA across every user and device in an organisation. KeeperPAM centralises secrets in a secure vault and can be configured to automatically rotate credentials. Keeper also provides secure remote infrastructure and database access without exposing credentials. Detailed reporting, real-time alerts and dark web monitoring enable organisations to quickly detect weak or compromised credentials to mitigate potential threats.
Paragraph 62: Timely Information About Vulnerabilities	**Have access to correct and timely information about vulnerabilities and establish an appropriate procedure to take mitigating measures.** Keeper's comprehensive Risk Dashboard provides admins with an instant overview of user activity and overall security status including weak or reused passwords or credentials that have been found on the dark web.
Paragraph 85: Supply Chain Security	**Manage supply chain security and relationships with suppliers.** Keeper Secrets Manager provides a fully managed cloud-based solution to store, access and rotate secrets, eliminating the uncontrolled distribution of confidential information within your environment. This includes passwords, API keys, database password keys, certificates and other sensitive data.
Paragraph 89: Cyber Hygiene Practices for Users	**Establish strong cyber hygiene practices, from zero-trust principles to identity and access management.** Keeper manages access permissions and monitors the activity of all users in an organisation through a combination of RBAC, secure credential storage, session management, MFA integration, and detailed auditing and reporting. Keeper centralises the management of privileged accounts for efficient access control, employs RBAC to ensure users have access only to what they need for their roles, securely stores credentials in encrypted vaults, monitors and records sessions for security and compliance, enhances security with MFA, and provides comprehensive audit trails for all privileged user actions.
Paragraph 98: End-to-End Encryption for Public Communications Providers	**Leverage end-to-end encryption to increase security.** Keeper is a zero-knowledge security provider. Zero knowledge is a system architecture that guarantees the highest levels of security and privacy. Encryption and decryption of data always occurs locally on the user's device. Keeper is the most secure, certified, tested and audited password security platform in the world. Keeper has the longest-standing SOC2 compliance and ISO27001 certification in the industry and complies with the EU-U.S. Data Privacy Framework ("EU-US DPF"), the UK Extension to the EU-US DPF and the Swiss-US Data Privacy Framework ("Swiss-U.S. DPF") as set forth by the US Department of Commerce.
Paragraph 102: Mandatory Incident Reporting	**Incidents must be reported within 24 hours of notification.** Keeper's Advanced Reporting and Alerts Module notifies admins of events with more than 200 event types for custom reporting with integrations to push notifications to Slack, Teams, email and many other preferred messaging solutions via webhook.