Special Report

Analysis of the DORA and NIS 2 Regulations in the Context of Enterprise Cybersecurity in the EU

SECFENSE

secfense.com

Introduction:

Legal changes in the area of cybersecurity. What awaits European entrepreneurs?

The role of technology in business and social life is growing. With it, the threat of cyberattacks increases. With this in mind, the European Union has developed new regulations to protect financial institutions and organizations operating in areas that are key to the functioning of states. The DORA regulation and the NIS 2 directive entered into force in 2023.

Who do they concern, what do they require? We know that the interpretation of regulations may raise doubts, especially since it is often difficult to find specific recommendations regarding the technologies that should be implemented. That's why we asked the experts of the Law4Tech Foundation to help us read the provisions of DORA and NIS 2. We have prepared this e-book based on their report.

You will find their basic information about the new legal acts, a description of the obligations arising from them, data on the persons responsible for implementation, and the penalties that organizations face for failure to comply with the new requirements.

Although DORA and NIS 2 avoid recommending specific technologies that increase security, they contain provisions indicating the need to implement strong authentication mechanisms. What are they, and how do you painlessly implement them in your organization? Explanations are also provided in this document.

We cordially invite you to read,
Secfense Team

What new legal acts are coming into force?

At the beginning of 2023, new cybersecurity and digital resilience regulations entered into force, aimed at increasing the protection of critical digital infrastructure in the financial sector and increasing the level of cybersecurity in the European Union.

The two key documents underpinning these changes are the Digital Operational Resilience Act (DORA) and NIS 2 (the Network and Information Security Directive).

DORA is a Regulation.

It binds in its entirety, and it is there directly used in all European Union countries. It entered into force on January 16, 2023, and applies from January 17, 2025.

NIS 2 is a Directive.

It requires implementation into national law through an act. It also allows for freedom to specify it more precisely at the national level. The implementation deadline is October 17, 2024.

What is DORA? Who does it apply to? What are the requirements? organizations?

What is DORA?

The DORA (Digital Operational Resilience Act) regulation is intended to increase the operational resilience of the financial sector. Applies to financial institutions and their ICT service providers (technology information and communication) obligation to use appropriate risk management measures, security testing, incident notification, and cooperation with supervisory authorities.

These organizations must decide for themselves what level of protection they will have in their case, the most appropriate one. The assessment of the accuracy of such a decision rests with the supervisory authorities in Poland - the Polish Financial Supervision Authority.

What entities does DORA apply to?

The DORA regulation covers operating entities in the financial sector.

DORA applies to:

- ☑ Traditional financial sector institutions, such as banks, credit institutions, investment and payment companies or companies insurance.

- Entities in the field of digital finance, including FinTech, electronic money institutions, crypto-asset service providers, or crowdfunding platforms (financing service providers social media).

- Technology providers for financial sector institutions, cloud computing service providers, service providers in the field of information sharing, and other ICT service providers.

What requirements does DORA place on organizations?

The primary purpose of the DORA regulation is to protect financial sector institutions against cyberattacks and prepare them to restore their operations in the event of an incident. DORA requires organizations to, among other things:

- **Prepare a cybersecurity policy, including an assessment of risk and a list of actions that will allow for its effective minimization.**

- **Implementation of appropriate security measures (including encryption, authentication, access control, monitoring, and audit tools).**

- **Implementation of incident detection and management processes related to ICT.**

- **Preparation of action scenarios (continuity plans actions) in the event of a cyberattack or other type of incident safety.**

Who is an external ICT service provider?

One of the tools to increase the level of resilience of the financial sector is the introduction of regulations facilitating the supervision of ICT services provided by third parties.

Within the meaning of DORA, an external ICT service provider, i.e., an "ICT third-party provider," is an external entity that provides outsourced ICT services to financial institutions. ICT services include, among others, ICT services, including cloud services, data hosting, data analytics, or artificial intelligence, as well as accompanying services.

Importantly, DORA does not completely equate the obligations of financial sector entities with the obligations of external ICT service providers. Financial organizations are responsible for purchasing digital services, including cooperating with service providers. The regulation includes provisions that explicitly prohibit cooperation with suppliers that do not comply with DORA in certain areas. Therefore, we should expect an increase in the expectations of financial entities towards digital service providers. As a result, although ICT service providers will not be generally obliged to comply with the regulation, they will have to meet its guidelines.

What are the penalties for failing to comply with the new regulations?

Failure to comply with obligations under DORA may result in the imposition of administrative sanctions by state regulators. They shall be proportionate, effective, and dissuasive and shall depend, inter alia, on the seriousness and intentionality of the infringement.

Possible sanctions:

- **requiring the temporary or permanent cessation of any practice or conduct considered contrary to the provisions of the Regulation;**
- **taking all kinds of measures, including those of a nature monetary to ensure continued compliance with the requirements of legal entities by financial entities;**
- **requiring access to existing data transfer registers owned by a telecommunications operator;**
- **issuing public announcements, including making public information indicating the identity of a natural or legal person, and nature of the infringement.**

All of the sanctions provided under the DORA regulations can significantly impact a company's operations. They may even lead to the end of its functioning.

What is NIS 2? Who does it apply to? What are the requirements? organizations?

The NIS 2 Directive (Network and Information Systems Directive) is EU-wide cybersecurity legislation aimed at increasing the level of cyber resilience of organizations providing services that are key to the economy and society, such as energy, transport, water management, healthcare, and digital infrastructure.

NIS 2 establishes minimum security and incident notification requirements and introduces new mechanisms for international and national cooperation in the field of cybersecurity.

Which organizations are affected by NIS 2?

The NIS 2 directive applies to public and private entities, operating in key and important sectors, providing services or operating in the European Union and qualifying as at least medium-sized enterprises.

Key sectors:

- energy (including electricity, heating or cooling, oil, gas, hydrogen)
- transport (including air transport, rail transport, water transport, and road transport)
- Banking
- financial market infrastructure
- Healthcare
- drinking water sector
- sewage
- digital infrastructure
- ICT service management (business-to-business)
- public administration space

Important sectors:

- postal and courier services, waste management
- production, processing and distribution of chemicals
- production, processing, and food distribution
- production (including: production of medical devices and medical devices for in vitro diagnostics, production of computers, electronic and optical products, production of electrical devices, production of machines and devices, production of motor vehicles, trailers and semi-trailers, production of transport equipment)
- digital services
- research

The size-cap rule in NIS 2

The directive introduced a uniform criterion determining which entities fall within its scope of application. The size-cap rule indicates that NIS 2 applies to medium-sized or larger organizations. However, Member States are entitled to extend the scope of national rules to certain small and micro-enterprises if they play a key role in society, the economy, or specific sectors or types of services.

Which companies are considered medium, small, and micro-enterprises? The number determines whether companies belong to a given category of employees, annual turnover, and annual balance sheet total.

Medium-sized enterprises employ fewer than 250 people, their annual turnover does not exceed EUR 50 million, and the annual balance sheet total does not exceed EUR 43 million. Small enterprises employ fewer than 50 employees, and their annual turnover or balance sheet total does not exceed EUR 10 million. Micro-enterprises employ fewer than 10 employees whose annual turnover or balance sheet total does not exceed EUR 2 million.

What requirements does NIS 2 place on organizations?

The NIS 2 Directive focuses on cybersecurity risk management measures. As required, key and essential entities are to implement appropriate and proportionate technical, operational, and organizational measures to manage the security risks of network and information systems and to prevent the impact of incidents on recipients of their services or on other services.

NIS 2, like DORA, considers the diversity of entities operating in the European market and introduces the principle of proportionality of protective mechanisms in relation to risk. However, NIS 2 requires key and important entities to adopt many basic cyber hygiene practices.

Basic cyber hygiene practices according to NIS 2:

- zero trust principle
- regular software update
- appropriate device configuration
- network segmentation
- identity and access management
- raising user awareness
- organization of training for employees
- spreading knowledge about cyber threats, phishing and techniques social engineering

What are the penalties for failing to comply with the new regulations?

NIS 2 does not contain specific regulations regarding sanctions. Their scope and method of enforcement depend on national legislation. However, sanctions must be effective, proportionate, and dissuasive.

However, supervisory authorities should be empowered at least to:

- perform on-site inspections and remote supervision,
- target security audits, as well as ad hoc audits in key entities in the event of a security incident,

- **request information on cybersecurity risk management measures, including a documented cybersecurity policy,**
- **request evidence of the implementation of the cybersecurity policy, such as the results of a security audit conducted by a qualified auditor,**
- **issue warnings regarding violations caused by given entities,**
- **issue binding orders, including in the field of incident prevention,**
- **order given entities to discontinue a given conduct,**
- **order the entities concerned to inform the natural or legal persons to whom they provide services about the existence of a cybersecurity threat,**
- **appoint an official to monitor a given entity,**
- **order the entities concerned to make their public inform about violations of the directive,**
- **impose of an administrative fine.**

The administrative fine provided for by the directive for key entities is EUR 10,000,000 or at least 2% of the total annual worldwide turnover in the previous financial year of the enterprise and for essential entities - EUR 7,000,000 or at least 1.4% of the total annual worldwide turnover in the previous financial year of the company's financial year.

In special cases, key entities may also expect the imposition of a temporary ban on performing management functions on a natural person performing the duties of the CEO or legal representative.

Financial institutions – what is more critical: DORA or NIS 2?

Entities in the banking sector are covered by both DORA and NIS 2, but can apply uniform security standards and incident notification defined by DORA, which is more detailed and tailored to the specifics of the financial sector.

Who is responsible for implementing DORA and NIS 2?

The entity responsible for implementing the provisions of the NIS 2 directive is the company's management board. Its task is to approve cybersecurity risk management measures and supervise their implementation. He must also participate in regular training to expand his knowledge and skills in assessing cybersecurity risk management practices and their impact on the services provided.

Under DORA, it is the financial entity's board of directors that determines, approves and oversees the implementation of all arrangements for the ICT risk management framework:

- **has ultimate responsibility for risk management related to ICT;**
- **introduces policies to ensure that high standards of data availability, authenticity, integrity and confidentiality are maintained;**
- **establishes clear roles and responsibilities for all ICT-related functions and establishes appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination in the performance of these functions;**

- **has full responsibility for defining and approving the financial entity's digital resilience operational strategy and ICT business continuity strategy and ICT response and recovery plans;**
- **approves the financial entity's internal plans ICT audits;**
- **allocates an appropriate budget to meet the financial entity's operational digital resilience needs for all types of resources, including appropriate ICT security awareness programs and operational digital resilience training;**
- **introduces reporting channels at enterprise level to obtain relevant information about ICT services.**

Board members must also regularly update their knowledge of ICT-related risks.

ICT management staff should also expect new responsibilities. Pursuant to the regulation, it has an important role in risk control and reporting, among other things, it is obliged to report to the management board at least once a year. It must focus on both technological and human aspects - it is important to build risk awareness and ensure that employees comply with cybersecurity rules.

According to lawyers:

The entity responsible for implementing the provisions of both NIS 2, like DORA, is the management body of the company. In the domestic context, this will usually be the company's management board capital company or partner of a partnership.

Tools that will help you adapt to new regulations

NIS 2 and DORA do not indicate specific tools that organizations should implement to increase their security. However, they require the use of appropriate strategies, policies, procedures, protocols, and technologies necessary to properly and adequately protect IT resources. In this context, securing access to systems, applications, databases, and other institutional resources, including the implementation of multi-factor authentication (MFA) and effective access management tools, becomes particularly important.

MFA – what is it, and how does it work?

Multi-factor authentication (MFA) is one of the best ways to protect yourself against phishing, social engineering, and credential theft. This is a mechanism that allows the user to increase the security of the login process. It requires the user to use at least two independent authentication factors.

A component can be something a person knows (knowledge component), something a person has (possession component), or who a person is (trait component).

- **Knowledge components include lock patterns, passwords, PINs, and personal questions such as your mother's maiden name.**
- **Possession assets are physical objects such as cryptographic keys or local authenticators (for example, smartphones).**
- **Feature components are based on biometric data and include face, fingerprint, and voice recognition.**

If an organization wants to improve application security, it can add more components or use more advanced authentication methods.

It is worth remembering that such popular passwords can be easily cracked. Therefore, multi-factor authentication (MFA) or two-factor authentication (2FA) is absolutely necessary to ensure that your online resources are properly protected.

Multi-factor authentication (MFA) can eliminate most cases of logging in using stolen data, as it provides additional protection and protects the authentication process against password spraying attacks and other password attacks.

MFA in the light of new regulations

DORA directly requires financial institutions to implement strong authentication mechanisms. The regulation uses precise wording: financial entities implement strong authentication mechanisms.

NIS 2 requires companies to implement appropriate security measures, including multi-factor authentication, where appropriate. At the same time, the directive indicates that entities should strive to implement technologies that improve cybersecurity, such as systems based on artificial intelligence or machine learning. Even more so, in the context of such far-reaching requirements, the strong authentication mechanism should be considered a basic protective mechanism that should constitute the foundation of the cybersecurity ecosystem in organizations.

According to lawyers:

It should be noted that under NIS 2, multi-factor or continuous authentication mechanisms are the basic tools for securing ICT systems.

Strong authentication mechanisms and the type of application

Neither DORA nor NIS 2 mandates that security measures be tailored to the type of web application or computer software.

DORA allows you to adjust the security of your applications to the scale of the financial institution's operations. Consequently, it is not the type of application used that determines the level of security but the scale of the entity's operations.

A similar principle was introduced in the NIS 2 regulation. The directive does not differentiate security levels based on the type of applications or software used. Each company decides on its own what security measures it will apply, including the nature and scale of activities. These decisions are verified each time by the supervisory authority.

Cryptographic key – what is it, and what does it mean? in security?

According to DORA, strong authentication mechanisms should be based on appropriate standards and special control systems and on measures to protect cryptographic keys. But what is a cryptographic key? It is a string of bits used to encrypt or decrypt information in cryptographic processes. Encryption can be symmetric or asymmetric.

In the case of symmetric encryption, the same security key is used to encrypt and decrypt information, which is not associated with the user (sender or recipient of the message), but with the operation being performed.

During asymmetric encryption, the algorithm uses two keys - one to encrypt the information (a public key that can be distributed) and another to decrypt it (a private key that should be confidential and stored securely).

Cryptographic keys are a mathematical tool, but a physical one can also be used in encryption. A U2F (Universal 2nd Factor) physical key is a device that serves as a second authentication factor. It works on the principle of asymmetric cryptography. The user has his or her own private key (stored safely on the device) and the corresponding public key (shared with the service).

How to quickly and effectively implement MFA in your organization?

There are many MFA solutions on the market, but often it takes many months to implement them in an organization. Additionally, it involves interference with the code.

Knowing these issues, Secfense developed the User Access Security Broker solution that enables you to deploy MFA on any application in 5 minutes and to roll out MFA across your organization in 7 to 14 days. The technology enables easy and quick implementation of any MFA, including the most effective today FIDO2, on any application without interfering with its code.

Thanks to UASB, every institution can use passwordless MFA, thus eliminating the risks associated with phishing, social engineering, and credential theft. The solution ensures the safety of stationary and remote employees, as well as customers and contractors. Because the Secfense solution works as a reverse proxy server and the entire implementation is simply the activation of learning mechanisms, there is no need to involve developers, suppliers, or any interference with the application source code.

How to effectively manage access to corporate information systems?

DORA and NIS 2 emphasize the importance of secure access to systems, applications, and databases. Enterprises and institutions obliged to implement new regulations should pay special attention to access management tools.

These include IAM (Identity and Access Management) systems, which enable secure management of access to data, applications, network resources, and services. Many large companies and organizations use several different IAM tools, if only because they match the applications used by employees.

However, migrating identities between individual IAM systems is problematic. It involves organizational chaos, overload of the helpdesk department, and additional costs. And maintaining various IAM solutions requires large budgets.

In response to these problems, Secfense created the Secfense IdP (identity provider) solution. This tool acts as a switch between different IAM systems and gives the company full control over its identity. Thanks to it, organizations can freely configure digital identity settings using various IAM tools and not limit themselves to a single provider. The new solution also allows you to implement additional security measures, such as passwordless authentication, conditional access, bot detection mechanism, or behavioral biometrics, regardless of whether these functions are included in the package the IAM manufacturer provides.

secfense.com