Let's go further

NIS2 and DORA compliance in EG

NIS2 and DORA compliance in EG

Contents

What are NIS 2 and DORA

NIS2 Directive and Digital Operational Resilience Act (DORA) are two key European Union regulations aimed at enhancing cybersecurity and operational resilience.

NIS2 Directive

The **NIS2 Directive** (Directive (EU) 2022/2555) is a European Union regulation aimed at achieving a high common level of cybersecurity across the EU. It replaces the original NIS Directive (Directive (EU) 2016/1148) and introduces stricter cybersecurity requirements for a broader range of sectors considered critical infrastructure.

It is applicable to medium and large enterprises from sectors viewed as critical infrastructure such as energy, transport, banking, health, public administration and others – to which many EG customers belong. It also directly applies to entities operating in digital infrastructure sectors, such as cloud service providers and managed service providers.

The NIS2 Directive came into effect on **January 16, 2023**, and then EU Member States transposed its measures into national law in various times. In Denmark it entered into force from **July 1, 2025**.

DORA

The **Digital Operational Resilience Act (DORA)** is an EU regulation designed to strengthen the IT security of financial entities such as banks, insurance companies, and investment firms, but also critical ICT providers in the financial sector. It aims to ensure that the financial sector in Europe remains resilient in the face of severe operational disruptions.

It is applicable to financial entities such as banks, insurance companies, investment firms. It is also applicable to critical ICT third-party service providers in the financial sector, that will be appointed by supervision authorities in the financial sector.

DORA entered into force on **January 16, 2023**, and is applicable from **January 17, 2025** (as an "EU regulation" it does not require additional country level laws to be passed to enter into force).

How are NIS2 and DORA applicable to EG and how EG is prepared

EG considers itself covered directly by NIS2 and launched a series of initiatives to ensure compliance with NIS2. As of date of entry into force in Denmark, EG is prepared and meets the requirements of NIS2.

In case of DORA, given the type of services and solutions that EG offers to financial sectors, EG does not consider itself to be nominated as a critical ICT provider in financial sector. However, the goal of EG is to give its financial sector customers the confidence that EG is a trusted partner keeping to the highest standards of information and cyber security. Therefore, as part of our compliance efforts, we completed initiatives that will allow our financial sector customers to satisfy their needs regarding initial assessment and ongoing supervision of security level in EG.

How EG addresses key NIS2 and DORA compliance topics

ICT Risk Management

We have implemented robust ICT risk management frameworks to identify, assess, and mitigate risks associated with our digital services. Our risk management processes are regularly reviewed and updated to ensure they remain effective in addressing emerging threats.

Risk Assessments are the basis for establishing the security strategy and selection of adequate security mechanisms, including requirements for our systems and policies. The implementation of security mechanisms and compliance with requirements is monitored for all EG products and internal infrastructure.

Incident Management and Reporting

Our incident response capabilities are designed to detect, respond to, and recover from cybersecurity incidents quickly and effectively. We have established clear procedures for reporting and managing incidents that may impact the security and resilience of our services. We are prepared to use communication channels with relevant authorities to ensure timely reporting of incidents as required by the regulations. We also have provisions to report significant incidents and threats to our customers, as required by NIS2.

Third-Party Risk Management

We conduct thorough due diligence on our third-party service providers on entering contracts with them, in order to ensure they meet our high standards for security and resilience. Our partners are also periodically or constantly monitored regarding their security, depending on their criticality level for EG.

Business Continuity and Disaster Recovery

We are ensuring the availability and recovery times suitable for the diverse products that EG offers. We are constantly monitoring, testing and working on optimization of our Disaster Recovery and Business Continuity measures.

Security Testing, including Penetration Tests

In EG we run an internal penetration testing program through which we periodically test effectiveness of our security measures, both for EG products as well as internal infrastructure. This is supplemented by ad hoc external penetration tests commissioned from renowned suppliers.

Our products and internal infrastructure are also covered by other techniques of security testing, such as vulnerability scans, application scans, external infrastructure scans as well as software composition analysis.

Other NIS2 Baseline Security Measures

We made sure that we have adequate security measures in place in line with the requirements of NIS2. More information about our security measures in different areas can be found in the document "Description of Security in EG" that we share with our customers in our website.

Audits, Certifications and Compliance

EG is committed to offering customers a strong compliance framework as well as advanced tools and security measures. Our goal is to build trust of our customers and be transparent in how we manage information and cyber security as well as compliance with various regulations, including GDPR, NIS2 and DORA. We fully understand the needs of our customers to perform their due diligence on EG, therefore, we provide the following resources to support our customers:

- Central EG operations (including centrally managed infrastructure, central internal IT and cybersecurity and compliance functions) as well as selected EG products are yearly audited for ISAE 3402 and ISAE 3000 certifications.
- Selected EG products have ISO 27001 certifications.
- We share with our customers a whitepaper describing security measures undertaken by EG ("Description of security in EG").

- We share with our customers our Information and Cyber Security Policy presenting the foundational security rules followed by EG in development and maintenance of products.

This information can be found in EG website. Additional resources and product-specific questions may be available upon discussion with your EG account manager or support.