BarentsKrans

Navigating NIS2 and Cybersecurity Act

Increase in Cybersecurity and Risk Management

The Network and Information Security (**NIS2**) Directive and the Cybersecurity Act aim to improve cybersecurity and resilience of essential services in EU member states. NIS2 significantly expands the scope of the current NIS Directive by covering more sectors. It also sets stricter and more elaborate security standards and incident reporting requirements.

Contact

Marc Elshof
attorney-at-law | partner

T: +31 70 376 06 87
M: +31 6 46 376 108
marc.elshof@barentskrans.nl

Sectors under NIS2 and the Cybersecurity Act

NIS2 Directive
The deadline for EU member states to transpose the NIS2 into their national law is 17 October 2024. In the Netherlands, the Cybersecurity Act implements NIS2. It is expected to take effect in 2025 The NIS2 and the Cybersecurity Act apply to entities qualifying as an **Essential Entity** or an **Important Entity**.

Essential Entities

- Entities (including affiliates) with more than 250 employees or an annual turnover exceeding EUR 50 million and an annual balance sheet exceeding EUR 43 million, operating within one of the sectors below:
  - Energy
  - Transport
  - Banking
  - Infrastructure Financial market
  - Healthcare
  - Drinking water
  - Digital infrastructure
  - Managers of ICT services
  - Wastewater
  - Government services
  - Local governments
  - Space
- Qualified trust service providers, top-level domain name registries and DNS service providers
- Medium-sized providers of public electronic communications networks or of publicly available electronic communications services
- Public administration entities
- Operators of Essential Services, as identified by an EU member state
- Companies identified as critical entities under the Critical Entities Resilience Directive
- Companies identified as Essential Entities by an EU member state

Important entities

- Entities not qualifying as Essential Entities, operating within one of the sectors below:
  - Energy
  - Transport
  - Banking
  - Infrastructure Financial market
  - Healthcare
  - Drinking water
  - Digital infrastructure
  - Managers of ICT services
  - Wastewater
  - Government services
  - Local governments
  - Space
  - Postal and courier services
  - Waste management
  - Manufacture, production and distribution of chemicals
  - Food production, processing and distribution
  - Manufacture
  - Digital providers
  - Research

Obligations under NIS2

Governance by management bodies

The management bodies of Essential and Important Entities must approve the cyber cybersecurity risk-management measures taken by those entities and oversee their implementation. Members of the management bodies can be held personally liable for infringements.

Members of the management body of Essential and Important Entities are required to follow training, and shall encourage those entities to offer similar training to their employees on a regular basis.

The aim is that employees gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Duty of care minimisation risk management

Essential and Important Entities must take appropriate and proportionate technical, operational and organisational measures to manage risks and prevent or minimise the impact of incidents. These measures include at least:

- Policies on risk analysis and system security;
- Incident handling;
- Business continuity;
- Supply chain security, taking into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures;
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- Policies/procedures to assess effectiveness of cybersecurity;
- Basic cyber hygiene practices and cybersecurity training;
- Cryptography and encryption policies and procedures;
- Human resources security, access control policies and asset management; and
- Use of multi-factor authentication or continuous authentication solutions.

Reporting obligations

Essential and Important Entities have to notify the competent national authority of any significant incident that has a significant impact on the provision of their services. An incident is significant if:

- It has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; or
- It has affected or can affect other entities by causing considerable material or non-material damage.

Essential and Important Entities have to notify the competent national authority of a significant incident:

- Within 24 hours after becoming aware of the incident, including whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
- Within 72 hours after becoming aware of the incident, including an update of the initial warning and an initial assessment of the severity, impact and the indicators of the compromise; and
- Within one month after the update notification, a final report. This report should include a description of the incident, type of threat and root cause, the measures taken and whether the significant incident has a cross-border impact.

Implementing Regulation

Implementing Regulation 2024/2690 provides further details on the technical and methodological requirements for the measures NIS2 requires. The Implementing Regulations also provides guidance to determine when incidents should be notified.

Representative

Entities providing domain name registration services, DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, providers of online search engines, and providers of social networking services platforms, which are not established in the EU but offer services in the EU, have to designate a representative in the EU. The representative must be established in one of the EU members states where the services are offered.

Supervisory Authorities and Enforcement

Supervisory authorities

- NIS2 requires member states to designate national supervisory authorities.
- The Cybersecurity Act designates Ministries as supervisory authorities for the sectors NIS2 oversees:

Enforcement

- NIS2 gives national supervisory authorities various enforcement powers, including:
  - Compliance orders;
  - Binding instructions;
  - Security audit implementation orders;
  - Threat notification orders to entities' customers
  - Charge of periodic penalty payments as long as obligations under the Cybersecurity Act are not met.

Administrative fines

For Essential entities

- Anticipatory and reactive supervision by national supervisory authorities;
- Administrative fines of up to € 10,000,000, or 2% of the global annual revenue, whichever is higher.

For Important Entities

- Reactive supervision by national supervisory authorities;
- Administrative fines of up to € 7,000,000, or 1.4% of the global annual revenue, whichever is higher.

Relevant Ministry by Sector

Ministry of Climate Policy and Green Growth

- Energy

Ministry of Economic Affairs

- Digital infrastructure
- ICT services management (business-to-business
- Postal and courier service
- Manufacture
- Digital providers
- Space

Ministry of Economic Affairs

- Banking
- Infrastructure Financial market

Ministry of the Interior and Kingdom Relations

- Government

Ministry of Infrastructure and Water Management

- Transport
- Drinking water
- Wastewater
- Waste management
- Manufacture, production and distribution of chemicals

Ministry of Health, Welfare and Sport

- Heathcare
- Manufacture

Ministry of Agriculture, Fisheries, Food Security and Nature

- Food production, processing and distribution