New rules on digital security in 2025 – implementation of EU directives in Norway – is your business prepared?

Kjetil Haare Johansen
Partner

Ketil Sellæg Ramberg
Partner

Hugo-A. B. Munthe-Kaas
Partner, Head of Compliance

Lars Albert Jøstensen
Lead Lawyer

New rules on digital security in 2025 – implementation of EU directives in Norway – is your business prepared?

In December 2023, the new Digital Security Act was passed. The law is based on the EU's new requirements for digital security, and will, together with a regulation, implement the EU's directive on security in network and information systems, initially through the so-called NIS1 directive.

The Cyber Security Act has not yet entered into force, but will enter into force in 2025, when the Regulations on Cyber Security, which are now on public consultation by the Ministry of Justice and Public Security, have been adopted. The deadline in the public consultation is 11 December 2024.

At the same time, the EU's legislative work is progressing rapidly, and the EU adopted a new directive on network and information systems – the NIS2 Directive – as early as 2022, which will replace NIS1 in its entirety. The NIS2 directive must also be implemented in Norway, and is now in the process of being incorporated into the EEA Agreement, which is the first step. Nevertheless, in the proposal for new regulations to the Cyber Security Act, the Ministry has sought to take into account some of the extended requirements and obligations under the NIS2 Directive.

The new regulations, which are expected to enter into force during 2025, will impose new and stricter requirements on providers of essential services. It will also have implications for customers of such providers, and for companies that are not directly subject to the Digital Security Act. Data center operators are one example of such businesses. At the same time, NSM – the Norwegian Security Authority - will have new and expanded powers of enforcement, and will potentially be able to impose administrative fines on companies of up to 4% of the total annual turnover in the previous financial year.

Are you prepared for these new demands and obligations?

The new rules will mean that the cybersecurity agenda will have to sail to the top of the priority list for many companies.

In the EU, NIS2 should have been implemented in the member states by 24 October this year, but so far the implementation is according to schedule, where only a few of the EU member states have so far met the requirements. When NIS2 becomes part of the EEA Agreement and its implementation is in place in the EU, the requirements and obligations will be much more extensive. However, many companies, as customers, already set requirements for suppliers' compliance with NIS2 obligations, regardless of the status of implementation in individual countries in the EU/EEA.

The requirements are extensive and will have a significant impact on the requirements for companies' management systems, their risk assessments, for security measures and incident reporting for suppliers (and customers) of digital services and for companies with socially important functions.

The purpose of the Cyber Security Act is to help ensure basic requirements for digital security in enterprises of particular importance to society by preventing, detecting and counteracting undesirable incidents in networks and information systems that are used to deliver essential services and digital services. The Act sets requirements for digital security and notification in the event of incidents that have a significant impact on the service delivery, and specifies the scope of application in terms of the sectors to which it applies. If you do not know whether you are covered or not, or whether you are indirectly influencing, now is the time to investigate this.

Who will be covered by the requirements of the Regulations?

The proposed regulations specify who will be covered by the Digital Security Act and the Regulations. Those who are covered will be providers of, for example:

- online search engines,
- cloud service providers,
- online marketplaces, as well as

- providers of essential services in:
  - Energy
  - Transport,
  - Health
  - Water supply
  - banking and financial market infrastructure, and
  - Digital infrastructure.

In principle, activities on the continental shelf, the economic zone and the adjacent zone are not covered, and the rules do not in principle apply to Norwegian upstream petroleum activities, including onshore facilities that are assumed to be excluded, but main tank storage facilities for petroleum-based fuels will, for example, be covered. Norwegian upstream petroleum activities will nevertheless be covered and subject to the rules –longer term.

The NIS2 directive will also expand industries and sectors that will be subject to the requirements of the Digital Security Act with regulations.

As a general rule, physical security in data centres will not be regulated by the Digital Security Act, but by the new E Com Act, but enterprises that are covered by the Digital Security Act, and that may use data centres, must nevertheless ensure that they have sufficient security in their own value chain, including for data centres and external suppliers that are used.

Providers of air navigation services, airport operations, commercial transport airlines, railways, metros and trams, traffic management and road surveillance, eCall alarm centres, coastal traffic monitoring, ports and port facilities, shipping companies, the health and care sector, systems for requisitioning medicines and other medical products, water supply, top-level domains, and internet interconnection points are also covered.

Enterprises that have fewer than 50 employees and that have an annual turnover or annual total balance sheet that does not exceed NOK 100 million will not be covered in principle, unless a decision is made whether the Act should nevertheless apply to them.

What are the requirements?

The proposal requires that covered companies must establish management systems for digital security, carry out risk assessments, and ensure incident management and notification within 24 hours of a cyber incident.

The management systems shall be based on "recognised standards", without this being specified in the Regulations. The management systems must be made known to the enterprise's employees, subcontractors, and other suppliers who perform work for or on behalf of the enterprise. In this respect, it may be worth taking into account that long and complex supply chains can in themselves constitute a particular exposure and vulnerability to cyber attacks.

Based on the risk assessments to be carried out, a risk management plan must be drawn up, and necessary organisational, technological, physical security measures must be taken, as well as the necessary security measures for personnel. Requirements for technical security measures will be to have written instructions for

routines and procedures, two- or multi-factor authentication for access to networks and information systems, access control to the content of networks and information systems based on service needs and measures for segmentation of services based on a principle of minimum rights, and measures to maintain the service in the form of a sufficient power supply, any emergency supply of electricity, as well as implementing measures for robust network access, security measures for personnel, as well as using confidentiality or confidentiality declarations, and doing follow-up and control of subcontractors.

In the event of incidents, notification must be made within 24 hours, with a requirement to update the notification within 72 hours, and with the submission of an incident report to NSM – the National Security Authority within one month of the first notification.

Furthermore, the proposed regulations contain provisions on the sharing of confidential information, regardless of whether it concerns technical devices and procedures and/or about operational or business matters that it would be of competitive importance to keep secret. The proposed regulations also contain certain provisions on the processing of personal data.

New legal basis for enforcement added to the National Security Authority (NSM)

Violation of the rules in the Digital Security Act with regulations can result in major financial sanctions in the form of fines (violation fines) up to 4% of the annual turnover. For public enterprises, the non-compliance fine can be set at a maximum of up to 25 times the basic amount, which results in a fine in the order of about NOK 3 million.

NSM can also demand information from businesses and demand access to premises in order to enforce the regulations, as well as NSM can make decisions, order tenderers that any regulatory violations must be rectified, as well as make decisions on coercive fines to ensure that orders are complied with.

Need more information?

If you need more information about NIS2 in particular, you can find more information about this here: NIS2 (Network and Information Systems Directive) | DLA Piper

DLA Piper can also offer a review of the regulations and how best to secure your business through access to our subject matter experts, both nationally, in the Nordic region and internationally.

If you want such a review, please contact:

- **Ketil S. Ramberg** - IPT (inkl. GDPR)
- **Lars Albert Jøstensen** - Insurance and Cyber Security
- **Hugo Munthe-Kaas** - Compliance
- **Kjetil Haare Johansen** - EU/EEA Regulatory