LOVDATA

Digital Security Regulations (Digital Security Regulations)

Date	FOR-2025-06-20-1131
Ministry	Ministry of Justice and Public Security
Entry into force	01.10.2025
Legal basis	ACT-2023-12-20-108-§2 , ACT-2023-12-20-108-§3 , ACT-2023-12-20-108-§6 , ACT-2023-12-20-108-§9 , ACT-2023-12-20-108-§13 , ACT-2023-12-20-108-§18
Announced	23.06.2025 at 10.50
Short title	Digital Security Regulations

Legal basis: Established by Royal Decree of 20 June 2025 pursuant to Act of 20 December 2023 No. 108 on digital security (Digital Security Act) Sections 2 , 3 , 6 , 9 , 13 and 18. Promoted by the Ministry of Justice and Public Security.
EEA references: EEA Agreement Annex XI No. 5cpa (Directive (EU) 2016/1148) and No. 5cpaa (Regulation (EU) 2018/151).

Chapter overview:

Chapter 1. Introductory provisions

§ 1. *Providers of essential services*

Providers of socially important services pursuant to the Digital Security Act, Section 2, first paragraph, letter a , and Section 6 are

1. KBO units, cf. the Power Emergency Preparedness Regulations, Section 2-1, second paragraph.

2. businesses that, by individual decision, are wholly or partly subject to the Power Emergency Response Regulations, Section 1-3, second paragraph
3. main tank system for petroleum-based fuel
4. air navigation service
5. commercial airports and service providers within the security restricted area of a commercial airport
6. airlines operating commercial transport with AOC in Norway
7. infrastructure management and traffic management of the national railway network
8. passenger transport exceeding 375,000 train kilometres per year, including cross-border transport
9. freight transport exceeding 500,000 train kilometres per year, including cross-border transport
10. infrastructure management, traffic management and train operation of metro and tram systems exceeding 12.5 million annual passenger journeys
11. traffic management and monitoring of the TEN-T road network
12. the most important road network in areas with annual daily traffic of over 20,000
13. emergency centers for eCall
14. national databases containing road or traffic information
15. traffic management and monitoring of coastal traffic
16. ports or port facilities that have a cargo throughput of more than 100,000 tonnes per year over a five-year period
17. ports or port facilities that handle more than 100,000 passengers per year over a five-year period
18. shipping companies that have ships with regular calls or that transport at least five percent of the number of passengers or cargo in a port as mentioned in points 16 and 17
19. The Ministry of Health and Care Services with its subordinate agencies, enterprises and other publicly owned enterprises, which constitute the national health preparedness
20. services offered by the regional health authorities
21. central systems for requisitioning and dispensing of medicines and other medical products
22. health and care services offered by a municipality with more than 50,000 inhabitants or more than 20,000 users who depend on the service, and the service cannot be transferred or relieved by other services
23. water supply system according to the Drinking Water Regulations Section 3 letter k , which treats at least 2000 m^3 per day
24. central registry of Norwegian top-level domains (.no)
25. recursive name service that, on average per 30 days, answers more than 15,000 domain name system requests per second
26. internet interconnection points
27. banks that the Ministry of Finance has decided to consider as systemically important in Norway, cf. CRR/CRD regulations section 30
28. enterprises that Finanstilsynet considers to be of significant importance to the Norwegian capital market.

§ 2. *Exceptions for small businesses*

Requirements for digital security for providers of digital services pursuant to Section 15 and the notification obligation pursuant to Section 17 do not apply to providers of digital services that have fewer than 50 employees and that have an annual turnover or annual total balance sheet that does not exceed 10 million euros.

§ 3. *Application to Svalbard*

The Digital Security Act also applies to Svalbard.

§ 4. *Decision that the Digital Security Act shall also apply to other providers of socially important services*

The responsible ministry may, in special cases, decide that the Act shall also apply in whole or in part to providers of essential services other than those mentioned in Section 1. The National Security Authority may make decisions pursuant to the first sentence with regard to enterprises that are not covered by any ministry's area of responsibility.

§ 5. *Registration of providers of essential public services*

Providers of a service of public importance must promptly report to the National Security Authority and the supervisory authority information about

a. business name, organization number and contact information
b. the service
c. social sector
d. in which other countries is the service offered
e. affected geographical area
f. changes to information mentioned in letters a to e.

Chapter 2. Digital security requirements for providers of essential services

§ 6. *Safety management system*

A provider of a socially important service shall establish and maintain a security management system that includes digital security. The management system shall be documented and included as part of the overall business management. Roles and responsibilities for digital security shall be defined, designated and documented.

The safety management system shall be based on recognized standards and contribute to

a. prevent incidents
b. uncover events
c. handle incidents
d. correct and restore security in networks and information systems in the event of incidents
e. Continuously manage and monitor that the objectives in letters a to d are achieved.

All activities necessary to establish and maintain an appropriate level of safety shall be included in the safety management system. The activities shall be documented and made known to personnel with a duty need.

The business manager is responsible for ensuring that the business has a reasonable level of security within the scope of the Digital Security Act . The security management system must be approved by the business manager and reviewed at least annually with the aim of improving the business's security work.

§ 7. *Risk assessment*

A provider of an essential service must prepare, maintain and document risk assessments.

The risk assessments shall be of such a scope that the provider can identify organizational, technological, physical and personnel security measures that safeguard the purposes in Section 8, second paragraph . In the event of changes in the business that may affect security, the provider shall assess the risk that the changes entail.

The risk assessments should at least describe:

a. the company's network and information systems and the importance these have for the delivery of the essential service
b. what events the company's network and information systems may be exposed to
c. what vulnerabilities are associated with the company's network and information systems
d. the consequence of events
e. the extent to which the business depends on other businesses to function properly.

§ 8. *Risk management*

Based on the risk assessments in Section 7 , a provider of a socially important service must have a plan for managing risk. As part of the risk management, the provider must implement organizational, technological, physical and personnel security measures to reduce risk and maintain a reasonable level of security.

The security measures shall, as a minimum, aim to contribute to a secure platform, secure operation and maintenance, as well as secure incident management and recovery.

§ 9. *Organizational security measures*

A provider of a socially important service must prepare written instructions, routines and procedures for digital security. The governance documents must be adapted to the size, complexity and risk profile of the business.

A provider of a socially important service must have updated action plans that can be implemented if the risk changes or an incident occurs, cf. Section 13 .

The management documents and action plans pursuant to the first and second paragraphs shall be made known to personnel who perform tasks for or on behalf of the enterprise and who may have access to the enterprise's network and information systems.

§ 10. *Technological security measures*

Based on the risk assessment pursuant to Section 7 , a provider of a socially important service must implement technological security measures that are adapted to the scope, complexity, operating environment, user environment, function and risk of the enterprise's network and information systems.

Technological security measures shall at least include:

a. strong authentication for access to networks and information systems
b. management and control of access to the company's network and information systems
c. measures for segmentation of networks and services based on the principle of least privilege
d. measures to ensure that networks and information systems can handle various types of disruptions and be restored within a reasonable time without significant reduction in the quality of service
e. measures to ensure that networks and information systems have sufficient capacity to withstand overload and equipment failure
f. measures to ensure that networks and information systems are continuously developed, including that updates are quality assured, installed and tested on an ongoing basis
g. Security monitoring of networks and information systems to detect incidents.

If one or more of the measures in the second paragraph cannot be implemented, this shall be approved by the head of the establishment. The justification for the exception shall be documented in the safety management system. The supervisory authority shall be informed of the exception.

§ 11. *Physical security measures*

A provider of a socially important service must implement physical security measures to maintain adequate security in networks and information systems.

Physical security measures shall at least include:

a. measures to prevent unauthorized persons from gaining access to locations and physical and technical infrastructure that networks and information systems use or rely on
b. measures to identify and protect buildings, rooms and adjacent areas that are important for the security level of networks and information systems that support the essential public service
c. measures to safeguard external dependencies, including data communication and power supply
d. measures to detect incidents with a negative impact on the security of networks and information systems.

§ 12. *Safety measures for personnel*

A provider of a socially important service must implement necessary security measures for employees, suppliers and contractors who may have access to the company's network and information systems by ensuring

a. that access to premises and access to networks and information systems is granted based on roles, tasks, responsibilities and service needs, and follow up to ensure that personnel do not have more access than necessary
b. that the personnel mentioned in this paragraph have been made aware of relevant security measures, that they have sufficient expertise in security and are provided with the necessary training when needed.

When an employment relationship or service ends, a provider of a socially important service must ensure that the person leaving no longer has access to the company's network and information systems.

§ 13. *Incident management and emergency preparedness*

A provider of a socially important service must have a contingency plan for handling incidents and notification pursuant to Section 17. The provider must consider relevant contingency measures and tightening of existing security measures that can be quickly implemented if necessary.

When the provider's network or information system is exposed to an incident, the nature and scope of the incident shall be identified. The provider shall implement the necessary countermeasures and actions to restore the secure state of the network and information system.

A provider of a socially important service must prepare, maintain and document emergency plans and conduct exercises to test the plan and develop the company's competence to handle incidents.

§ 14. *Obligation to follow up*

A provider of a socially important service must ensure that suppliers and others who perform work that may affect the security of networks and information systems and who perform work for or on behalf of the business, perform the work in a manner that ensures that the requirements for proper security are met.

A provider of a socially important service shall, through agreement or in another appropriate manner, make the security measures applicable to suppliers as mentioned in the first paragraph, to the extent necessary to maintain a reasonable level of security.

Chapter 3. Digital security requirements for providers of digital services

§ 15. *Security management measures for digital service providers and criteria for determining whether an incident should be considered to have a significant impact*

The EEA Agreement, Annex XI, No. 5cpaa (Regulation (EU) 2018/151) applies as a regulation with the adaptations that follow from Annex XI, Protocol 1 to the Agreement and the Agreement in general.

Chapter 4. Common provisions

§ 16. *Response environments*

The National Security Authority is the national response environment for handling incidents under the Digital Security Act .

The responsible ministry may designate response environments that can assist a provider of a socially important service in handling incidents within the sectors mentioned in the Digital Security Act, section 2, first paragraph, letter a . The National Security Authority shall be informed of the designation.

Anyone who performs or has performed work or assignments for a response environment is obliged to prevent unauthorized persons from gaining access to or knowledge of what the person concerned learns about someone's personal circumstances or operating and business secrets in connection with the work or assignment. Any duty of confidentiality imposed on the person concerned by law or otherwise does not prevent the response environments from exchanging information with each other to the extent necessary to perform the tasks assigned in or pursuant to the Digital Security Act .

A response environment must comply with relevant requirements arising from or pursuant to the Digital Security Act and in addition ensure

a. redundant and secure communication solutions, with clearly defined and clearly communicated communication channels to members and partners
b. secure locations for workplaces, infrastructure and systems
c. emergency preparedness and continuity solutions that ensure that notification and incident management can be performed and handed over between multiple parties, with sufficient resources for continuous availability and access to redundant systems and locations.

Furthermore, the response environments shall contribute to the national response environment's mission solution and as a minimum

a. contribute to a comprehensive cyber risk picture, by having an overview of and reporting on incidents, vulnerabilities and threats within one's own area of responsibility at all times
b. Disseminate notifications about cyber risks and incidents to relevant recipients
c. respond to incidents within their own area of responsibility
d. contribute to public-private collaboration, including by promoting the use of standards for incident management, risk management, and taxonomy.

The national response environment shall also, as a minimum,

a. coordinate and advise on national efforts for intentional serious cyber incidents
b. maintain a timely and national cyber risk picture
c. contribute to a comprehensive situational understanding in cyber incidents
d. participate in the CSIRT Network, as well as be able to participate, where appropriate, in other international collaborative networks.

§ 17. *Duty to notify*

A notification pursuant to sections 8 and 11 of the Digital Security Act shall be sent to the supervisory authority with a copy to the National Contact Point. The notification shall be sent no later than 24 hours after a provider of a socially important service became aware of the incident. The notification shall contain information about

a. provider's name and contact information
b. affected service
c. the incident, including possible causes and consequences
d. number of affected users
e. the event's effects in other countries.

The information in the notification must be updated within 72 hours.

Within one month of the notification referred to in the first paragraph being sent, the provider shall provide the supervisory authority with an incident report. The incident report shall contain updated information on the circumstances referred to in the first paragraph and the remedial measures that have been implemented.

The supervisory authority may require status updates and the information necessary to perform assigned tasks.

§ 18. *Sharing of confidential information*

The supervisory authority may share confidential information received upon notification pursuant to Section 17 with national and international actors when necessary to achieve the purpose of the Digital Security Act . The recipient shall be informed if the shared information is subject to a duty of confidentiality.

In the event of a risk of serious incidents, the National Security Authority shall inform relevant national and international actors about the risk and possible measures.

§ 19. *Processing of personal data*

Businesses and authorities covered by the Digital Security Act may process personal data, including personal data as mentioned in Articles 9 and 10 of the General Data Protection Regulation , when necessary to perform tasks in or pursuant to the Digital Security Act .

Personal data shall be processed for specific, explicit and legitimate purposes, including to:

a. implement security measures
b. handle incidents, including assistance
c. exercise the duty to notify
d. receive notifications
e. perform tasks as a response environment
f. perform duties as a national contact point
g. supervise.

The processing of personal data and the interference with privacy shall not be more extensive than is necessary to achieve the purpose.

§ 20. *National contact point for security in networks and information systems*

The National Security Authority is the national single contact point for the security of network and information systems pursuant to Directive (EU) 2016/1148 Article 8(3) . The national contact point shall ensure cooperation between Norwegian authorities and relevant authorities in other EU/EEA countries and participate in the cooperation group and the CSIRT network established pursuant to Articles 11 and 9 of the Directive. The national contact point should forward reports of incidents to national contact points in other affected Member States. The national contact point shall routinely send a quarterly summary report to the cooperation group, on the number of reports received and the nature of the reported incidents, including the type of security breach, severity or duration. Where appropriate, the national contact point should consult with the authority pursuant to the Personal Data Act .

Section 21. *Supervision of providers covered by the Digital Security Act*

The responsible ministry designates authorities to supervise businesses within its own sector. For businesses without a supervisory authority, the National Security Authority is the supervisory authority.

The supervisory authority may use assistance from others in connection with the supervision.

§ 22. *Limitation on the right to supervise providers of digital services*

Supervision of providers of digital services can only be carried out if the supervisory authority receives information about violations of provisions provided in or pursuant to the Digital Security Act and the supervisory authority finds it necessary.

§ 23. *Duty to provide information and access to premises*

The supervisory authority may set deadlines and the form in which the information pursuant to Section 14 of the Digital Security Act must be provided.

Necessary documentation and information shall be made available to the supervisory authority. The person being supervised or his representative may be required to be present during the inspection.

§ 24. *Violation fine*

The supervisory authority may impose a fine for violation pursuant to Section 17 of the Digital Security Act . The fine for violation accrues to the treasury and may amount to up to 25 times the basic amount in the National Insurance Scheme or four percent of the business's annual turnover in the previous financial year if it concerns an enterprise. The highest amount constitutes the upper limit. In any case, the fine for violation may not exceed NOK 50 million.

When assessing whether a violation fine should be imposed, and when determining the amount, particular emphasis shall be placed on:

a. the nature of the violation, including its duration
b. how serious the violation is
c. guilty plea
d. the provider's profit and turnover
e. the actual impact of the infringement on the market
f. the size of the affected market
g. whether the offender has had a leading or passive role in the infringement.

Other factors that may be relevant when imposing and determining fines include:

a. whether measures have been implemented
b. whether the provider could have prevented the violation through guidelines, instructions, training, control or other measures
c. whether the provider has assisted the authority in connection with the investigation of the violation.

Decisions on fines for violations are grounds for enforcement. If a lawsuit is filed against the state to challenge the decision, the enforcement is suspended.

Chapter 5. Final provisions

§ 25. *Entry into force*

The regulations come into force on 1 October 2025.