Print date: July 16, 2025

LAW No. 434 of 06/05/2025 (Current)

Act on measures to ensure a high level of cybersecurity (NIS 2 Act)

Ministry: Ministry of Social Security and Emergency

Journal number: Ministry of Community Safety and Emergency Management, journal number 202577

Act on measures to ensure a high level of cybersecurity (NIS 2-the law)1)

WE FREDERICK THE TENTH, by the Grace of God King of Denmark, do hereby:

The Danish Parliament has adopted and We have ratified by Our consent the following law:

Chapter 1

Scope, jurisdiction, definitions, etc.

Section 1. The Act applies to public and private entities covered by Annexes 1 and 2 to the Act, cf. however, paragraphs 2-5 and 7.

Subsection 2. The Act does not apply to entities to the extent that they are covered by the Act on Enhanced Emergency Preparedness in the Energy Sector. The Act does not apply to entities to the extent that they are covered by the Act on Security and Emergency Preparedness in the Telecommunications Sector, cf. however section 1, subsection 2 of this Act. Furthermore, the Act does not apply to entities designated pursuant to section 333, subsection 1 of the Financial Business Act.

Subsection 3. The Act does not apply to entities where sector-specific EU legislation and any national implementation thereof has at least the same effect as the provisions of sections 6, 12, 13 and 15.

Subsection 4. The Act does not apply to public administration units that carry out their activities within the framework of national security, public safety, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.

Subsection 5. The relevant minister may, within his or her area, decide to exempt specific entities if the entities carry out activities within the scope of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or exclusively provide services to public administration entities carrying out these activities, from the obligations in sections 6, 8, 12, 13, 15 and 16, insofar as these activities or services are concerned. If entities carry out exclusively activities or exclusively provide services of the type referred to in the first sentence, the relevant minister may also decide to exempt these entities from the obligations pursuant to sections 9 and 10, cf. however subsection 6.

Subsection 6. Rules may not be laid down pursuant to subsection 5 where an entity functions as a trust service provider.

Subsection 7. The relevant minister may, after negotiation with the Minister for Public Safety and Emergency Preparedness, lay down rules to the effect that the Act shall also apply, in whole or in part, to public administration units at local level and educational institutions, respectively.

§ 2. Danish jurisdiction includes entities that are covered by the scope of the Act and that are established in Denmark, cf. however, subsection 2.

Subsection 2. DNS service providers, top-level domain name administrators, entities providing domain name registration services, and providers of cloud computing services, data center services, content delivery networks, managed services, managed security services, online marketplaces, online search engines and platforms for social networking services, respectively, that have their principal place of business in Denmark, cf. subsection 3, fall under Danish jurisdiction.

Subsection 3. An entity as referred to in subsection 2 shall be deemed to have its principal place of business in the European Union in the Member State where the decisions relating to the measures for managing cybersecurity risks are predominantly taken. If such a Member State cannot be determined, or if such decisions are not taken in the European Union, the principal place of business shall be deemed to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the principal place of business shall be deemed to be in the Member State where the establishment of the entity in question with the largest number of employees in the European Union is located.

Subsection 4. If an entity as referred to in subsection 2 is not established in the European Union, but provides services within the Union, including in Denmark, the entity must appoint a representative established in one of the Member States of the Union where the entity's services are provided. If the representative is established in Denmark, the entity falls under Danish jurisdiction. If a representative has not been appointed pursuant to subsection 1, the entity shall be deemed to fall under the jurisdiction of the Member States where the services are provided.

Section 3. In this Act, the following definitions apply:

1) Central contact point: The authority that exercises the liaison function to ensure cross-border cooperation between the Danish authorities, authorities in other Member States of the European Union and the institutions of the European Union and to ensure cross-sectoral cooperation between the national competent authorities.

2) Cloud computing service: A digital service that enables on-demand administration and provides broad remote access to a scalable and flexible pool of shareable computing resources, including where these resources are distributed across multiple locations.

3) Cybersecurity: The activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats.

4) Cyber threat: Any potential circumstance, event or action that could damage, disrupt or otherwise have a negative impact on network and information systems, the users of such systems and other persons.

5) Data center service: A service that includes structures or groups of structures intended for the central storage, interconnection and operation of IT and network equipment that provides data storage, data processing and data transport services, as well as all facilities and infrastructures for energy distribution and environmental control.

6) Digital service: Any service in the information society, i.e. any service that is normally provided for payment and that is provided electronically at the individual request of a service recipient.

7) DNS Service Provider: An entity that provides
(a) publicly available recursive domain name translation services for internet end-users; or
(b) authoritative domain name translation services for third party use, with the exception of root names; servers.

8) Domain Name System (DNS): A hierarchical distributed naming system that allows Internet services and resources to be identified so that end-user equipment can use Internet routing and connectivity services to reach those services and resources.

9) Entity: A natural or legal person established and recognised as such under the national law of the place where it is established and which may exercise rights and be subject to obligations in its own name.

10) Entity providing domain name registration services: A registrar or an agent acting on behalf of registrars, such as a provider or reseller of privacy or proxy registration services. nests.

11) Research organisation: An entity whose primary objective is to carry out applied research or development with a view to exploiting the results of that research for commercial purposes. This does not include educational institutions.

12) Incident: An event that endangers the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by or accessible through network and information systems.

13) Incident management: Any action and procedure aimed at preventing, detecting, analyze and contain or respond to and recover from an incident.

14) ICT process: Activities carried out to design, develop, deliver or maintain an ICT product or an ICT service.

15) ICT product: An element or group of elements in network and information systems.

16) ICT service: A service which consists wholly or mainly of the transmission, storage, retrieval or processing of information using network and information systems.

17) Content Delivery Network: A network of geographically distributed servers for the purpose of ensuring high availability of, access to or rapid delivery of digital content and digital services to internet users on behalf of content and service providers.

18) Qualified trust service: A trust service that meets the requirements laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

19) Qualified trust service provider: A trust service provider that provides one or more qualified trust services and has been granted the status of qualified trust service provider by the supervisory body pursuant to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

20) The management body:

a) For companies covered by the Companies Act, the management body is

i) the board of directors of companies that have a management board and a supervisory board,

(ii) the management board in companies that have only one management board, and

(iii) the management board in companies that have both a management board and a supervisory board.

b) For companies covered by the Act on Certain Commercial Companies, the management body is

i) the board of directors of companies that have a management board and a supervisory board,

(ii) the management board in companies that have only one management board, and

(iii) for companies that have neither a board of directors nor a management board, the management body that has a competence corresponding to the general perception of the competence of a board of directors or a management board.

c) For public authorities, the management body is the highest administrative management of the authority.

21) Network and information system:

(a) An electronic communications network, which means transmission systems, whether or not based on a permanent infrastructure or centralised management capacity, and, where applicable, switching and routing equipment and other resources, including network elements that are not active, which enable the transmission of signals by wire, radio waves, fibre optics or other electromagnetic means, including satellite networks, fixed terrestrial networks (circuit and packet switched, including in the Internet) and mobile networks, electricity cable systems, to the extent that they are used for the transmission of signals, networks used for radio and television broadcasting and cable television networks, regardless of the type of information transmitted.

b) Any device or group of connected or related devices, one or more of which, by means of a program, performs automatic processing of digital data.

c) Digital data stored, processed, retrieved or transmitted by elements in letters a and b with for the purpose of their operation, use, protection and maintenance.

22) Near-miss: An event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by or accessible through network and information systems, but which was successfully prevented or which did not occur.

23) Online marketplace: A service that uses software, including a website, part of a website or an application, operated by or on behalf of the trader, which enables consumers to conclude distance sales contracts with other traders or consumers.

24) Online search engine: A digital service that allows users to enter queries to search essentially all websites or all websites in a particular language based on a query on any subject using a keyword, voice search, phrase or other input, and that displays results in any format where information about the desired content can be found.

25) Social networking service platform: A platform that enables end-users to connect with each other across different devices, in particular through chats, posts, videos and recommendations.

26) Representative: A natural or legal person established in the European Union who is expressly designated to act on behalf of a DNS service provider, a top-level domain name administrator, an entity providing domain name registration services, or a provider of cloud computing services, of data centre services, of content delivery networks, of managed services, of managed security services, of online marketplaces, of online search engines or of social networking service platforms not established in the European Union and who can be contacted by a competent authority or a Computer Incident Response Team (CSIRT) at the location of the entity, with regard to that entity's obligations under the NIS 2 Directive.

27) Risk: The potential for loss or disruption resulting from an event, expressed as a combination of the magnitude of such loss or disruption and the probability of the event occurring.

28) Security of network and information systems: The ability of network and information systems to withstand, at a given level of security, any event that could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by or accessible through these network and information systems.

29) Vulnerability: A weakness, susceptibility or flaw in ICT products or services that can be exploited of a cyber threat.

30) Trust service: An electronic service that is normally provided for a fee and consists of:
(a) generation, verification and validation of electronic signatures, electronic seals or electronic time stamps or electronic registered delivery services and certificates related to services,
(b) generation, verification and validation of certificates for website authentication; or
c) preservation of electronic signatures, seals or certificates related to these services.

31) Trust service provider: A natural or legal person who provides one or more trust services, either as a qualified or non-qualified trust service provider.

32) Top-level domain name administrator: An entity that has been delegated a specific top-level domain and is responsible for administering the top-level domain, including the registration of domain names under the top-level domain and the technical operation of the top-level domain, which includes the operation of its name servers, the maintenance of its databases and the distribution of top-level domain zone files to name servers, regardless of whether any of these operations are performed by the entity itself or outsourced, but not situations where top-level domain names are used only by an administrator for his own use.

33) Managed Security Service Provider: A managed service provider that performs: or provides assistance with activities related to cybersecurity risk management.

34) Managed service provider: An entity that provides services related to the installation, administration, operation or maintenance of ICT products, networks, infrastructure, applications or other network and information systems through assistance or active management, carried out either at the customers' premises or remotely.

35) Significant cyber threat: A cyber threat that, based on its technical characteristics, can be assumed to have the potential to have a serious impact on an entity's network and information systems or on the users of the entity's services by causing significant physical or non-physical damage.

Essential units

Section 4. Entities of a type covered by Annex 1 of the Act are considered to be significant entities if the entity meets one of the following conditions, cf. however, paragraphs 2 and 3:

1) The entity employs 250 people or more.
2) The entity has an annual turnover of more than EUR 50 million and an annual balance sheet total of more than EUR 43 million. euros.

Subsection 2. Municipalities and regions are considered significant entities if they perform tasks as providers of public electronic communications networks or providers of publicly available electronic communications services for a commercial purpose and meet at least one of the following conditions:

1) The entity employs 50 people or more.
2) The entity has an annual turnover exceeding EUR 10 million and an annual balance sheet total exceeding EUR 10 million. euros.

Subsection 3. Regardless of their size, the following entities are considered to be significant entities:

1) Qualified trust service providers and top-level domain registrars, as well as DNS service providers.
2) Public administration units under the central government.
3) Units identified as critical units under the CER Act.
4) Entities that have been identified as operators of essential services in accordance with Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures to ensure a high common level of security of network and information systems across the Union (NIS I Directive), cf. however section 5(2).

5) Other units of a type covered by Annex 1 or 2 of the Act, where at least one of the following conditions are met, cf. however, section 5(2):
   a) The entity is the only provider in Denmark of a service that is essential for the maintenance of critical societal or economic activities.
   b) A disruption of the service provided by the entity could have a significant impact on public safety or public health.
   (c) A disruption of the service provided by the entity could pose a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact.
   d) The entity is critical due to its specific importance at national or regional level for the sector or type of service in question or for other interdependent sectors in Denmark.

Subsection 4. The relevant minister may, after negotiation with the Minister for Public Safety and Emergency Preparedness, Cabinet shall lay down further rules on when entities are covered by subsection 3, no. 5.

Important devices

Section 5. Entities of a type covered by Annex 1 or 2 of the Act are considered to be important entities if the entity does not meet the criteria for being significant entities pursuant to Section 4 and the entity meets at least one of the following conditions:

1) The entity employs 50 people or more.
2) The entity has an annual turnover of more than EUR 10 million and an annual balance sheet total of more than EUR 10 million. euros.

Subsection 2. The competent authority may decide that an entity, regardless of size, which is covered by section 4(3)(4) or (5), shall be considered to be a significant entity.

Subsection 3. Notwithstanding subsection 1, nos. 1 and 2, trust service providers that do not meet the criteria are considered to be essential units, to be important units.

Chapter 2

Measures to manage cybersecurity risks

§ 6. Essential and important entities shall take appropriate and proportionate technical, operational and organisational measures to manage the risks to the security of network and information systems that these entities use for their operations or to provide their services, and to prevent incidents or minimise their impact on recipients of their services and on other services. The measures shall include at least the following:

1) Policies for risk analysis and information system security.
2) Incident management.
3) Business continuity, including backup management and disaster recovery and crisis management.
4) Supply chain security, including security-related aspects concerning the relationships between the individual entity and its direct suppliers or service providers.
5) Security in connection with the acquisition, development and maintenance of network and information systems more, including handling and disclosure of vulnerabilities.
6) Policies and procedures for assessing the effectiveness of cybersecurity management measures health risks.
7) Basic cyber hygiene practices and cybersecurity training.
8) Policies and procedures regarding the use of cryptography and, where applicable, encryption.
9) Personnel security, access control policies and asset management.
10) Use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications, and secured emergency communication systems within the entity, where applicable.

Subsection 2. An entity that does not comply with one or more of the requirements referred to in subsection 1 for the measures or rules on requirements for measures laid down pursuant to subsection 3 shall, without undue delay, take all necessary, appropriate and proportionate corrective measures.

Subsection 3. The relevant minister may, after negotiation with the Minister for Public Safety and Emergency Preparedness, Cabinet shall lay down further rules on measures pursuant to subsection 1.

Section 7. The measures taken by a significant or important entity on the basis of Section 6(1) and (2) and rules laid down pursuant to Section 6(3) must be approved by the entity's management body. The management body shall supervise the implementation of the measures.

Subsection 2. The members of a significant or important entity's management body shall participate in relevant courses on managing cybersecurity risks and encourage similar courses to be offered to the entity's other members.
employees.

Section 8. The relevant minister may, after negotiation with the Minister for Public Security and Emergency Preparedness, lay down rules requiring essential and important entities to use specific ICT products, services and processes certified under a European cybersecurity certification scheme to demonstrate compliance with certain requirements in Section 6(1) or rules on measures laid down pursuant to Section 6(3). The product may be developed by the essential or important entity or purchased from third parties.

Chapter 3

Registration and notification obligations

§ 9. DNS service providers, top-level domain name administrators, entities providing domain name registration services, and providers of cloud computing services, data center services, content delivery networks, managed services, managed security services, online marketplaces, online search engines and social networking service platforms shall register with the relevant competent authority and in this connection provide the following information:

1) Device name.
2) The address of the entity's principal place of business and its other places of business in the European Union or, if it is not established in the Union, the representative appointed pursuant to Section 2(4), 1st sentence.

3) The relevant sector, sub-sector and type of entity, cf. Annex 1 or 2 of the Act.
4) Up-to-date contact information, including email addresses, IP ranges and phone numbers on the device and contact information for any designated representative pursuant to Section 2(4).
5) The Member States of the European Union where the entity provides services.

Subsection 2. The information pursuant to subsection 1 must be submitted no later than 3 months after the entity is covered by the Act.

Subsection 3. In the event of changes in the information provided pursuant to subsection 1, the entity shall provide the relevant competent authority no later than 3 months after the date of the change.

§ 10. Essential and important entities and entities providing domain name registration services shall register with the relevant competent authority and in this connection provide the following information, cf. however, section 9:

1) Device name.
2) Address and up-to-date contact information, including email addresses, IP ranges and telephone numbers.
3) The relevant sector and sub-sector to which the entity is subject, cf. Annex 1 or 2 of the Act.
4) A list of the other Member States of the European Union where the entity provides services that are covered by the scope of Article 2 of the NIS 2 Directive.

Subsection 2. The information pursuant to subsection 1 must be submitted no later than 2 weeks after the entity is covered by the Act.

Subsection 3. In the event of a change in the information provided pursuant to subsection 1, the entity must provide the relevant competent authority no later than 2 weeks after the date of the change.

Database of domain name registration data

§ 11. Top-level domain name administrators and entities providing domain name registration services shall: maintain a separate database containing accurate and complete domain name registration data.

Subsection 2. The database pursuant to subsection 1 shall contain information on the following:

1) The domain name.
2) The registration date.
3) The name, email address and telephone number of the data subject.
4) Email address and telephone number of the point of contact that administers the domain name, if the point of contact is different from the registrant.

Subsection 3. The top-level domain name administrators and entities providing domain name registration services shall establish policies and procedures, including verification procedures, to ensure that the databases contain accurate and complete information. The policies and procedures shall be made publicly available.

Subsection 4. Top-level domain name administrators and entities providing domain name registration services shall, without undue delay after the registration of a domain name, make domain name registration data that is not personal data publicly available.

Subsection 5. Top-level domain name administrators and entities providing domain name registration services shall, upon request and after a specific assessment of necessity, grant legitimate access seekers access to specific domain name registration data, including personal data. Requests shall be responded to no later than 72 hours after receipt of the request. Top-level domain name administrators and entities providing domain name registration services shall establish and publish policies and procedures for access to data.

Subsection 6. Top-level domain name administrators and entities providing domain name registration services shall cooperate in complying with the obligations set out in subsections 1-5, with a view to avoiding double collection of domain name registration data.

Subsection 7. The competent authority may issue prohibitions or injunctions to top-level domain name administrators and entities providing domain name registration services to ensure compliance with the requirements under subsections 1-6 or regulations issued pursuant to subsection 8.

Subsection 8. The Minister for Digitalisation may lay down further rules on requirements for policies and procedures pursuant to subsections 3 and 5.

Notification obligations

§ 12. Significant and important entities shall notify the relevant competent authority and the Computer Security Incident Response Team (CSIRT) of any significant incident. A notification shall contain information that makes it possible to determine any cross-border effects of the incident.

Subsection 2. An incident is considered to be significant if one of the following conditions is met:

1) The incident has caused or is capable of causing serious disruption of services or financial losses to the affected entity.

2) The incident has affected or is capable of affecting other natural or legal persons by causing significant physical or non-physical harm.

Subsection 3. The relevant minister may, after negotiation with the Minister for Public Safety and Emergency Preparedness, The Danish government may lay down more detailed rules on when an incident can be considered significant.

Section 13. Notification pursuant to Section 12(1) shall consist of the following and shall be made in the following manner:

1) An early warning, which shall indicate whether the significant incident is suspected of being caused by illegal or malicious acts or could have a cross-border impact, shall be sent without undue delay, and at the latest within 24 hours after the entity has become aware of the significant incident.

2) An incident notification, which shall update the information from the early warning, cf. no. 1, and provide an initial assessment of the significant incident, including its severity and impact and the indicators of compromise, where such exist, shall be sent without undue delay, and in any event within 72 hours after the entity has become aware of the significant incident, cf. however, subsection 2.

3) An interim report with relevant status updates is sent upon request from the CSIRT.

4) A final report shall be sent no later than 1 month after the transmission of the incident notification that is referred to in point 2. The report must contain the following:
   a) A detailed description of the incident, including its severity and impact.
   b) The type of threat or root cause that is likely to have triggered the incident.
   c) Applied and ongoing mitigation measures.
   d) The possible cross-border effects of the incident.

5) If the incident is still ongoing at the time of submission of the final report, cf. no. 4, the notifying entity must submit a status report at that time and a final report no later than 1 month after the incident has been handled.

Subsection 2. In the event of significant incidents, trust service providers must submit the notification pursuant to subsection 1, no. 2, without undue delay and no later than 24 hours after becoming aware of the significant incident.

Subsection 3. The CSIRT shall ensure that the notifying entity is provided with a response, including initial feedback on the significant incident, without undue delay and within 24 hours of receipt of the early warning, cf. subsection 1(1). Upon request from the entity, the CSIRT shall also provide guidance, operational advice on the implementation of possible mitigating measures and additional technical assistance.

Voluntary notifications

§ 14. Public and private entities may, regardless of whether they are not covered by the scope of the Act, notify the CSIRT of incidents, near-misses and cyber threats.

Subsection 2. The CSIRT shall process notifications pursuant to subsection 1 in the same way as notifications received pursuant to section 13. The CSIRT may prioritize the handling of notifications received pursuant to section 13 over notifications pursuant to subsection 1.

Subsection 3. Notifications pursuant to subsection 1 are exempt from access to documents pursuant to the Act on Public Administration and access to party documents pursuant to the Public Administration Act.

Chapter 4

Notification and information about significant incidents

§ 15. Essential and important entities shall, without undue delay, inform the recipients of their services of: significant events that are likely to adversely affect the delivery of their services.

Subsection 2. Essential and important entities shall, without undue delay, inform recipients of their services potentially affected by a significant cyber threat of any measures or countermeasures that the recipients may take in response to such a threat. The entities shall also inform the recipients concerned of the significant cyber threat, where relevant.

Section 16. The relevant competent authority may, after consulting an entity affected by a significant incident, inform the public about the significant incident if the disclosure is necessary to prevent further spread of or to deal with the incident, or if disclosure of the incident is otherwise in the public interest.

Subsection 2. The competent authority may, in the situations referred to in subsection 1, decide that the relevant entity shall inform the public about the significant incident and determine how this information shall be provided.

Subsection 3. The CSIRT may, in accordance with the same criteria as in subsection 1, inform the public about significant events that may affect more than one sector.

Subsection 4. The CSIRT may, in accordance with the same criteria as in subsection 1, inform the public about significant incidents in other Member States.

Chapter 5

CSIRT tasks

§ 17. The CSIRT handles IT security incidents and carries out the tasks related thereto, including the following tasks in relation to significant and important units:

1) Upon request from a significant or important entity, to provide assistance regarding real-time or near-real-time Real-time monitoring of the unit's network and information systems.
2) Respond to incidents and provide assistance to affected entities in this regard.
3) Upon request from a significant or important entity, conduct a proactive scan of the entity's network and information systems used to provide the entity's services to detect vulnerabilities with a potentially significant impact.

Subsection 2. When performing tasks pursuant to subsection 1, the CSIRT may prioritize specific tasks based on a risk-based approach.

§ 18. The CSIRT ensures that natural and legal persons can report vulnerabilities in anonymized form.

Subsection 2. The Minister of Public Safety and Emergency Preparedness may lay down further rules on reporting, handling and disclosure pursuant to subsection 1.

§ 19. The CSIRT facilitates the voluntary exchange of information between entities in cybersecurity communities, including communities at the European level.

Subsection 2. Significant and important entities that join or withdraw from cybersecurity communities pursuant to subsection 1 shall notify the competent authority thereof.

Subsection 3. Public and private entities may, regardless of whether they are not covered by the scope of the Act, participate in the voluntary exchange of information between entities in cybersecurity communities pursuant to subsection 1.

Chapter 6

Supervision and enforcement

Section 20. The Minister for Public Safety and Emergency Preparedness shall, after negotiation with the relevant minister, lay down rules on which authority shall perform the function as competent authority within a given sector or sub-sector or for a specific type of entity, cf. Annex 1 or 2 to the Act. The Minister for Public Safety and Emergency Preparedness may, after negotiation with the minister exercising the authority in Section 1(7), lay down rules on which authority shall perform the function as competent authority for these entities.

Subsection 2. In order to ensure operational independence in the supervision of public administration, the Minister for Public Safety and Emergency Preparedness may, after negotiation with another minister, lay down rules to the effect that supervision of the Ministry for Public Safety and Emergency Preparedness, including subordinate authorities, is wholly or partly entrusted to the minister in question.

Subsection 3. The Minister for Public Safety and Emergency Preparedness may lay down rules on coordination, responsibility, distribution of tasks and exchange of information between the competent authorities and the competent authorities and the CSIRT, respectively, including in relation to incident notifications pursuant to Chapter 3 and supervision and enforcement pursuant to this Chapter.

Supervisory and control measures for significant entities

Section 21. The competent authorities shall supervise, in their respective areas, the compliance of significant entities with this Act and regulations issued pursuant to the Act. A competent authority may, as part of its supervision, apply the following supervisory measures to a significant entity:

1) Without a court order and against proper identification, carry out on-site inspections and external supervision, including random checks.
2) Conduct regular and targeted security audits or require the entity to have a qualified independent body conduct these audits and that the results thereof be made available to the competent authority.
3) Conduct security audits.
4) Perform security scans.
5) Require the provision of information necessary to assess the measures for the management of cybersecurity risks introduced by the affected entity.
6) Require access to data, documents and information necessary for the performance of the supervisory task, including for determining whether a matter is covered by this Act or regulations issued pursuant to the Act.
7) Require documentation of the implementation of cybersecurity policies.

Subsection 2. When applying the measures in subsection 1, nos. 5-7, the competent authority shall state the purpose thereof and specify what information is required to be provided, and how and in what form the information and material mentioned in subsection 1, nos. 5-7, shall be provided.

Enforcement measures for significant entities

Section 22. The competent authority may apply the following enforcement measures against a essential unit:

1) Issue warnings about the entity's violation of this law.
2) Issue binding instructions, including regarding measures necessary to prevent or remedy an incident and deadlines for implementing such measures and for reporting on their implementation, or order the entities concerned to remedy the identified deficiencies or violations of this Act.
3) Order the entity to take measures necessary to prevent or remedy a incident.
4) Issue orders and prohibitions to the unit to ensure compliance with the requirements set out in the Act or regulations issued pursuant to the Act.
5) Order the entity to notify the natural or legal persons to whom the entity provides services or for whom it carries out activities that may potentially be affected by a significant cyber threat of the nature of that threat and of any protective or remedial measures that the natural or legal persons may take in response to that threat.
6) Order the entity to implement the recommendations made in connection with a completed security audit.
7) Appoint a person responsible for supervising the unit's compliance with sections 6, 12, 13 and 15 and section 16(2) and regulations issued pursuant thereto, for a specified period.
8) Order the entity to publish, in non-anonymized form and in a specified manner, decisions on enforcement measures pursuant to nos. 1-5 and summaries of judgments or fines where a fine is imposed or adopted.

Section 23. If one or more of the enforcement measures imposed pursuant to Section 22, Nos. 1-4, have proven to be insufficient, the competent authority may set a deadline within which the significant entity must take the necessary measures to remedy the deficiencies or meet the requirements of the competent authority. If the measures are not taken within the specified deadline, the competent authority may decide on the following, cf. however, subsection 4:

1) To temporarily suspend a certification or approval in respect of part or all of the relevant services provided by the entity or activities carried out by the entity.
2) Temporarily prohibit any natural person with management responsibilities at the level of the CEO or the legal representative of the entity from exercising management functions in the entity in question.

Subsection 2. Suspensions or prohibitions imposed pursuant to subsection 1 may only be applied until the entity takes the necessary measures to remedy the deficiencies or meet the requirements that gave rise to the application of the measures.

Subsection 3. A decision pursuant to subsection 1 may not be appealed to another administrative authority, but may be appealed by the The entity or natural person to whom the decision relates is required to be brought before the courts.

Subsection 4. The provisions of subsections 1-3 do not apply to public administration units.

Subsection 5. The relevant minister shall, after negotiation with the Minister for Public Safety and emergency regulations on which certifications and approvals are covered by subsection 1, no. 1.

Supervision and control measures for important entities

Section 24. The competent authorities shall carry out reactive supervision of compliance by significant entities with this Act and regulations issued pursuant to this Act. As part of this supervision, a competent authority may, following indications that a significant entity is not complying or has not complied with this Act or regulations issued pursuant to this Act, apply the following supervisory measures:

1) Without a court order and against proper identification, conduct on-site inspections and subsequently remotely supervision.

2) Conduct targeted security audits or require the entity to have a qualified independent body conduct these audits and to make the results available to the competent authority.

3) Perform security scans.

4) Require the provision of information necessary to subsequently assess the measures for managing cybersecurity risks that the affected entity has put in place.

5) Require access to data, documents and information necessary for the performance of the supervisory task, including for determining whether a matter is covered by this Act or regulations issued pursuant to the Act.

6) Require documentation of the implementation of cybersecurity policies.

Subsection 2. When applying the measures in subsection 1, nos. 4-6, the competent authority shall state the purpose of the requirement and specify what information is required to be provided, and how and in what form the information and material mentioned in subsection 1, nos. 4-6, shall be provided.

Enforcement measures against key entities

Section 25. A competent authority may apply the following enforcement measures to a significant entity:

1) Issue warnings about the entity's violation of this law.

2) Issue binding instructions, including regarding measures necessary to prevent or remedy an incident and deadlines for implementing such measures and for reporting on their implementation, or order the entities concerned to remedy the identified deficiencies or violations of this Act.

3) Issue orders and prohibitions to the unit to ensure compliance with the requirements set out in the Act or regulations issued pursuant to the Act.

4) Require the entity to notify the natural or legal persons to whom it provides services or for whom it carries out activities that may potentially be affected by a significant cyber threat of the nature of that threat and of any protective or remedial measures that the natural or legal persons may take in response to that threat.

5) Order the entity to implement the recommendations made in connection with a completed security audit.

6) Order the entity to publish, in non-anonymized form and in a specified manner, decisions on enforcement measures pursuant to nos. 1-3 and summaries of judgments or fines where a fine is imposed or adopted.

Consultation of essential and important entities

Section 26. Before the competent authority decides to apply enforcement measures pursuant to sections 22, 23 or 25, the entity concerned shall be informed of the intended enforcement measures and the reasons therefor. The competent authority shall give the entity a reasonable period of time to submit observations, except in cases where the purpose of the measure would otherwise be defeated.

Chapter 7

Mutual assistance

Section 27. Where an entity provides services in more than one Member State of the European Union, or where the entity provides services in one or more Member States and the entity's network and information systems are located in one or more other Member States, the competent authorities shall cooperate with the competent authorities of the other Member States to the appropriate extent. The cooperation shall include the following:

1) The competent authorities shall notify, through the central contact point, the competent authorities of:
relevant Member States on the supervisory and enforcement measures applied.
2) The competent authorities may request the competent authorities of another Member State to apply supervisory and enforcement measures to entities in that country.
3) The competent authorities shall provide reasonable assistance to the competent authority of another Member State upon receipt of a reasoned request to that effect.

Subsection 2. The competent authorities may, by further agreement, carry out joint supervisory measures with competent authorities from other Member States of the European Union.

Subsection 3. If a request for mutual assistance is received, cf. subsection 1, concerning DNS service providers, top-level domain name administrators, entities providing domain name registration services, and providers of cloud computing services, data center services, content delivery networks, managed services, managed security services, online marketplaces, online search engines and social networking service platforms, appropriate supervisory and enforcement measures may be taken against the entity if it provides services or has a network and information system in Denmark.

Chapter 8

Disclosure of information, digital communication, implementing acts and operational independence

Section 28. The competent authorities may disclose information to the authorities of other Member States and to institutions of the European Union in order to carry out the tasks arising from this Act or regulations issued pursuant to this Act.

Section 29. The obligations laid down in this Act or in regulations issued pursuant to the Act do not include the provision of information the disclosure of which would be contrary to essential interests in the interests of national security, public safety or defence.

Subsection 2. Information received or originating from authorities in other EU Member States shall be treated as confidential if the issuing authority considers the information to be confidential in accordance with EU or national rules.

Section 30. The relevant minister may, after negotiation with the Minister for Public Security and Emergency Preparedness, lay down rules necessary to implement legal acts issued by the European Commission pursuant to the NIS 2 Directive.

Section 31. The Minister of Public Safety and Emergency Preparedness may lay down rules on digital communication, including the use of certain IT systems and special digital formats as well as digital signatures or the like.

Chapter 9

Punishment

§ 32. A fine shall be imposed on anyone who:
1) violates section 6, subsection 1 or 2, sections 9 or 10, section 11, subsections 1-6, section 12, subsection 1, section 13, subsection 1 or 2, or section 15,
2) fails to comply with a decision of a competent authority pursuant to section 23(1)(1) or (2),
3) fails to comply with an order or prohibition pursuant to section 22(1)(3-6) or section 25(1)(3-6),
4) fails to comply with a decision pursuant to section 16(2), section 21(1)(2) or (5-7), or section 24(1)(1)(2).
2 or 4-6, or
5) prevents the competent authorities from carrying out supervision in accordance with the provisions of section 21(1)(1)(1)-4, or section 24, subsection 1, nos. 1-3.

Subsection 2. Companies etc. (legal persons) may be held criminally liable in accordance with the rules in Chapter 5 of the Criminal Code.

Subsection 3. Regulations issued pursuant to the Act may stipulate a fine for violation of provisions of the regulations.

Chapter 10

Entry into force, transitional provisions and changes to other legislation

§ 33. The Act enters into force on 1 July 2025.

Subsection 2. No later than 3 years after the Act enters into force, the Minister of Public Safety and Emergency Preparedness shall prepare a report on the experience with the Act, which shall be submitted to the Folketing.

Subsection 3. The information pursuant to Section 9(1) and Section 10(1) must be submitted no later than 1 October 2025.

Subsection 4. Act No. 436 of 8 May 2018 on network and information security for domain name systems and certain digital services is repealed.

Subsection 5. Act No. 437 of 8 May 2018 on security in network and information systems for operators of significant internet exchange points, etc. is repealed.

Subsection 6. Act No. 440 of 8 May 2018 on security requirements for network and information systems within the healthcare sector is repealed.

Subsection 7. Act No. 441 of 8 May 2018 on security of network and information systems in the transport sector is repealed.

Chapter 11

Territorial determination

Section 34. The Act does not apply to the Faroe Islands and Greenland, but may by royal decree be brought into force in whole or in part for the Faroe Islands and Greenland with the amendments required by the Faroese and Greenlandic conditions respectively. The provisions of the Act may be brought into force at different times.

Given at Christiansborg Palace, May 6, 2025

Under Our Royal Hand and Seal

FREDERICK R.

/ Torsten Schack Pedersen

1) The Act implements Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive), EU Official Journal 2022, no. L 333, page 80.

Appendix 1

Sectors of particularly critical importance

Sector	*Sub-sector*	*Type of device*
1. Energy	a) Electricity	– Electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944 of the European Parliament and of the Council, which are responsible for 'supply' as defined in Article 2(12) of that Directive
		– Distribution system operators as defined in Article 2(29) of Directive (EU) 2019/944
		– Transmission system operators as defined in Article 2(35) of Directive (EU) 2019/944
		– Producers as defined in Article 2(38) of Directive (EU) 2019/944
		– Designated electricity market operators as defined in Article 2(8) of Regulation (EU) 2019/943 of the European Parliament and of the Council – Market participants as defined in Article 2(25) of Regulation (EU) 2019/943 providing services relating to aggregation, flexible electricity demand or energy storage as defined in Article 2(18), (20) and (59) of Directive (EU) 2019/944 – Charging station operators responsible for the management and operation of a charging station that provides a charging service to end-users, including in the name and on behalf of a mobility service provider
	b) District heating and cooling	– District heating or cooling operators as defined in Article 2(19) of Directive (EU) 2018/2001 of the European Parliament and of the Council
	c) Oil	– Oil pipeline operators
		– Operators of oil production facilities, refineries and processing plants, oil storage and oil transmission
		– Central storage units as defined in Article 2(f) of Council Directive 2009/119/EC

	d) Gas	– Utilities as defined in Article 2(8) of Directive 2009/73/EC of the European Parliament and of the Council
		– Distribution system operators as defined in Article 2(6) of Directive 2009/73/EC
		– Transmission system operators as defined in Article 2(4) of Directive 2009/73/EC
		– Storage system operators as defined in Article 2(10) of Directive 2009/73/EC
		– LNG system operators as defined in Article 2(12) of Directive 2009/73/EC
		– Natural gas undertakings as defined in Article 2(1) of Directive 2009/73/EC
		– Operators of natural gas refineries and processing plants
	d) Hydrogen	– Operators in hydrogen production, storage and transmission
2) Transportation	a) Air	– Air carriers as defined in Article 3(4) of Regulation (EC) No 300/2008, used for commercial purposes
		– Airport managing bodies as defined in Article 2(2) of Directive 2009/12/EC of the European Parliament and of the Council, airports as defined in Article 2(1) of that Directive, including the main airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council; and entities with associated installations at airports
		– Air traffic management and control operators providing air traffic control services as defined in Article 2(1) of Regulation (EC) No 549/2004 of the European Parliament and of the Council
	b) Railway	– Infrastructure managers as defined in Article 3(2) of Directive 2012/34/EU of the European Parliament and of the Council
		– Railway undertakings as defined in Article 3(1) of Directive 2012/34/EU, including operators of service facilities as defined in Article 3(12) of that Directive;

	c) Water	– Shipping companies that carry out passenger and transport of goods by inland waterways, on the high seas or in coastal waters as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council, with the exception of individual vessels operated by these shipping companies
		– Port operators as defined in Article 3(1) of Directive 2005/65/EC of the European Parliament and of the Council, including their port facilities as defined in Article 2(11) of Regulation (EC) No 725/2004; and entities operating installations and equipment in ports
		– Operators of maritime traffic services as defined in Article 3(o) of Directive 2002/59/EC of the European Parliament and of the Council
	d) Road transport	– Road authorities as defined in Article 2(12) of Commission Delegated Regulation (EU) 2015/962, responsible for traffic management, with the exception of public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity;
		– Operators of intelligent transport systems votes as defined in Article 4(1) of Directive 2010/40/EU of the European Parliament and of the Council
3. Banking		– Credit institutions as defined in Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council
4. Financial market infrastructure		– Operators of trading venues as defined in Article 4, point 24, of Directive 2014/65/EU of the European Parliament and of the Council
		– Central counterparties (CCPs) as defined in Article 2(1) of Regulation (EU) No 648/2012 of the European Parliament and of the Council
5. Health		– Healthcare providers as defined in Article 3(g) of Directive 2011/24/EU of the European Parliament and of the Council
		– EU reference laboratories referred to in Article 15 of the European Parliament

		Regulation (EU) 2022/2371 of the European Parliament and of the Council
		– Entities carrying out research and development activities relating to medicinal products as defined in Article 1(2) of Directive 2001/83/EC of the European Parliament and of the Council – Units manufacturing pharmaceutical raw materials and pharmaceutical preparations as referred to in Section C, Division 21, of NACE Rev. 2 – Entities that manufacture medical devices that it considers to be critical in a public health crisis ('list of critical medical devices for public health crises') within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council
6. Drinking water		– Suppliers and distributors of drinking water as defined in Article 2(1)(a) of Directive (EU) 2020/2184 of the European Parliament and of the Council, except for distributors for whom the distribution of drinking water is a non-essential part of their general activity of distributing other raw materials and goods
7. Wastewater		– Undertakings collecting, disposing of or treating urban, domestic or industrial waste water as defined in Article 2(1), (2) and (3) of Council Directive 91/271/EEC, with the exception of undertakings for which the collection, disposal or treatment of urban, domestic or industrial waste water is a non-essential part of their general activity
8. Digital infrastructure		– Internet exchange point providers tur – DNS service providers other than root name server operators – Top level domain name administrators – Cloud computing service providers – Data center service providers – Content delivery network providers – Trust service providers

		– Providers of public electronic communication network
		– Providers of publicly available electronic communications services
9. Business-to-business services management		– Managed service providers – Managed security service providers
10. Public administration		– Public administration units under the central government as defined by a Member State in accordance with national law
		– Public administration units at regional level as defined by a Member State in accordance with national law
11. The room		– Operators of terrestrial infrastructure owned, managed and operated by Member States or private parties and supporting the provision of space-based services, except providers of public electronic communications networks

Appendix 2

Other critical sectors

Sector	*Sub-sector*	*Type of device*
1. Postal and courier services		– Postal companies such as defined in Article 2(1a) of Directive 97/67/EC, including courier service providers
2. Waste management		– Undertakings carrying out waste management as defined in Article 3(9) of Directive 2008/98/EC of the European Parliament and of the Council, with the exception of undertakings for which waste management is not their main economic activity
3. Manufacturing, production and distribution of chemicals		– Companies that deal with with the manufacture of substances and distribution of substances or mixtures as referred to in Article 3, points 9 and 14, of Regulation (EC) No 1907/2006 of the European Parliament and of the Council, and undertakings engaged in the production of articles as defined in Article 3, point 3, of that Regulation from substances or mixtures
4. Production, manufacturing and distribution of food		– Food businesses as defined in Article 3(2) of Regulation (EC) No 178/2002 of the European Parliament and of the Council, engaged in wholesale distribution and industrial production and processing
5. Manufacturing	a) Manufacture of medical devices and in vitro diagnostic medical devices	– Entities manufacturing medical devices as defined in Article 2(1) of Regulation (EU) 2017/745 of the European Parliament and of the Council and entities manufacturing in vitro diagnostic medical devices as defined in Article 2(2) of Regulation (EU) 2017/746 of the European Parliament and of the Council, with the exception of entities manufacturing medical devices referred to in the fifth indent of point 5 of Annex I to this Directive
	b) Manufacture of computers and electronic and optical products	– Enterprises engaged in one of the economic activities covered by Section C, Division 26, of NACE Rev. 2

	c) Manufacture of electrical equipment	– Enterprises engaged in one of the economic activities covered by Section C, Division 27, of NACE Rev. 2
	d) Manufacture of machinery and equipment nec engaged in one of these	– Companies economic activities covered by Section C, Division 28, of NACE Rev. 2
	e) Manufacture of motor vehicles, trailers and semi-trailers – Companies carrying out one	of the economic activities referred to in Section C, Main Group pe 29, in NACE Rev. 2
	f) Manufacture of other means of transport	– Enterprises engaged in one of the economic activities covered by Section C, Division 30, of NACE Rev. 2
6. Digital providers		– Online marketplace providers
		– Online search engine providers
		– Social networking service platform providers
7. Research		– Research organizations