FINNISH LANGUAGE COLLECTION

Published in Helsinki on 7 April 2025

124/2025

Cybersecurity Act

In accordance with the decision of Parliament, it is provided that:

Chapter 1

General provisions

Section 1

Scope of application

This Act provides for the management of cybersecurity risks.

This Act implements measures to ensure a high common level of cybersecurity across the Union, Regulation (EU) No 910/2014 and Directive
amending Regulation (EU) 2018/1972 and repealing Directive (EU) 2016/1148
Directive (EU) 2022/2555 of the European Parliament and of the Council *(NIS 2 Directive).*

The implementation of the NIS 2 Directive in the public administration sector referred to in point 10 of Annex I to the said Directive is provided for in the Act on Information Management in Public Administration (906/2019).

Section 2

Definitions

For the purposes of this Act:

1) *the administrator of a domain name registry means* an entity that has been granted the right to administer a specific domain name and that, when administering it, is responsible for the registration of domain names in its below and its technical operation;

2) *data center service* means a service that comprises structures or groups of structures that:
is intended for the centralized maintenance, interconnection and control of IT equipment and network devices that provide data storage, processing and transmission services together
with all necessary equipment and infrastructure for electricity distribution and regulation of operating conditions;

3) *DNS service provider means* an operator that provides publicly available recursive domain name resolution services to Internet end users or authoritative domain name resolution services to third parties, excluding root name servers;

4) *vulnerability means* the weakness of information and communication technology products or services, a vulnerability or defect that could cause a cyber threat or anomaly;

HE 57/2024
LiVM 1/2025
EV 15/2025

Directive (EU) 2022/2555 of the European Parliament and of the Council (32022L2555), OJ L 333, 27.12.2022, p. 80

5) *management service provider means* an operator that provides services related to the installation, management, use or maintenance of ICT products, networks, infrastructure, applications or other communication networks and information systems referred to in paragraph 17, either on-site support or active maintenance carried out via remote connection.
in terms of;

6) *an approved trust service provider* for electronic identification and electronic on transaction-related trust services in the internal market and Directive 1999/93/EC repealing Regulation (EU) No 910/2014 of the European Parliament and of the Council *(eIDAS Regulation)* a qualified trust service provider as referred to in Article 3(20);

7) *cybersecurity* means the measures required to protect communication networks and information systems, to protect their users and other interested parties from cyber threats;

8) *cyber threat means* a situation, event or activity that, if realized, could damage or disrupt communications networks or information systems, the users of such systems and other persons or otherwise adversely affect them;

9) *trust service provider* means a trust service provider as defined in Article 3(19) of the eIDAS Regulation;

10) *cloud service means* a digital service that offers scalable, remote access for widespread use and a flexible set of shareable and need-based IT resources;

11) *by deviating from* an event that endangers communication networks and information systems the availability, authenticity, integrity or confidentiality of any stored, transmitted or processed information or services provided or accessible through them;

12) *incident handling means* actions and procedures aimed at preventing and detecting an incident, analyzing, limiting or controlling it, and recovering from it.
thence;

13) *risk means* the possibility of loss or disruption caused by an event, expressed as a combination of the magnitude of the loss or disruption and the probability of the event occurring;

14) *content delivery network means* a network of geographically distributed servers, which The aim is to ensure good accessibility of digital content and digital services, usability and rapid distribution to internet users by content and service providers;

15) *information security service provider means* a management service provider that operates in the field of cybersecurity to manage or provide support for oral risks;

16) *ICT service* from the European Union Agency for Cybersecurity ENISA and the Information and Regulation (EU) 2019/881 of the European Parliament and of the Council on cybersecurity certification of communication technologies and repealing Regulation (EU) No 526/2013 *(Cybersecurity Regulation)* information and communication technology referred to in Article 2(13) service;

17) *ICT product means* an information and communications technology product referred to in Article 2(12) of the Cybersecurity Regulation;

18) *supervisory authority means* the authorities mentioned in section 26;

19) *an online community platform* means a platform that allows end users to connect each other, share content, search for information and communicate with each other using a wide variety of terminal devices;

20) *online search engine means* an online search engine as referred to in Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services;

21) *in an online marketplace,* Chapter 6, Section 8 of the Consumer Protection Act (38/1978) an online marketplace referred to in paragraph 4;

22) *communication network and information system*

(a) the European Electronic Communications Code, adopted by the European Parliament and Council Directive (EU) 2018/1972 *(Telecommunications Directive)* as referred to in Article 2(1) electronic communications network;

b) a device or a group of devices connected or interconnected, one or more of which performs automatic processing of digital data using a program; and

(c) digital data stored in the systems referred to in points (a) and (b), processed, retrieved or transferred for the operation, use, protection or maintenance of these systems;

23) *security of a communication network and information system means* the ability of a communication network and information systems to protect themselves with a certain degree of certainty from events that may endanger the the availability, authenticity, integrity or confidentiality of any stored, transmitted or processed information or services provided or accessible through them;

24) *provider of publicly available electronic communications services means* a person who offers a communications service referred to in section 3, paragraph 37 of the Act on Electronic Communications Services (917/2014) to an undefined group of users;

25) *provider of public electronic communications networks* means a provider of electronic communications an online service referred to in Section 3, Paragraph 34 of the Act on Internet Services.

Section 3

Actors

This Act applies to a legal person and a natural person *(actor)* who:

1) carries out an activity referred to in Annex I or II or is an operator referred to in those Annexes; and 2) meets or

exceeds the medium-sized enterprises criteria set out in Article 2 of the Annex to Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises. conditions for companies and offers its services or carries out its activities in a In a Member State of the European Union.

This Act also applies to an operator, regardless of size, that is:

1) public electronic communications networks or publicly available electronic communications service provider;

2) trust service provider;

3) the administrator of the domain name register; or

4) DNS provider.

In addition, this Act applies to any operator, regardless of its size, that carries out an activity referred to in Annex I or II or is an operator referred to in the said Annexes, if:

1) it provides a service that is essential for maintaining critical functions in society or the economy and that is not provided by other operators;

2) a disruption in the service it provides would significantly affect public order, public safety or public health;

3) a disruption in the service it provides could cause significant systemic risk to the various particularly in areas where such disruption could have cross-border effects; or

4) it is critical because it is of particular importance at a national or regional level at the level of the sector or type of service concerned or of other interdependent sectors of a Member State of the European Union.

More detailed provisions on the criteria referred to in subsection 3 above may be issued by Government decree.

Article 3 of the Annex to the Recommendation referred to in paragraph 1, point 2 does not apply to the operator. 4 points.

Section 4

Scope limitations

Chapter 2 of this Act does not apply to activities or services provided for the purpose of national defence, national security, public order and safety, or the prevention, investigation and prosecution of crimes.

This Act does not apply to an operator who only offers the services referred to in subsection 1. service or service.

Notwithstanding subsections 1 and 2 above, the Act applies to an operator who is a trust service provider.

This Act does not apply to an operator that is subject to the digital resilience of the financial sector. and regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 of the European Parliament and of the Council Regulation (EU) 2022/2554 *(DORA Regulation)* does not apply pursuant to Article 2(4) thereof.

This Act does not apply to an operator who carries out an activity referred to in Annex I or II. is random and minor.

This Act applies to a municipality referred to in the Municipalities Act (410/2015) only in Annex I or II for the activities referred to.

The provisions of this Act that oblige the provision of information shall not apply if the provision of information would endanger national defence or national security or would be contrary to: important benefit associated with it.

Section 5

Relationship to other legislation

If another law or the provisions or regulations issued under it contain provisions from this law deviating requirements for managing cybersecurity risks or reporting significant deviations and the requirements have effects at least as great as those provided for in this Act obligations, they shall apply in place of the corresponding provisions of this Act.

If a European Union regulation or a Commission regulation issued under the NIS 2 Directive The regulation requires the operator to implement cybersecurity risk management measures to control or report significant deviations, and the requirements are provisions with effects at least equivalent to the obligations laid down in this Act shall apply in place of Chapters 2, 4 and 5 and Section 41 of this Act.

The data security of the processing of personal data is regulated by the data protection act of natural persons. Regulation (EU) 2016/679 of the European Parliament and of the Council of 15 December 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as *the General Data Protection Regulation,* and in the Data Protection Act (1050/2018).

In addition to what is provided in this Act regarding the powers of the supervisory authority, the permit The cancellation is subject to the provisions of the Act on the Supervision of the Electricity and Natural Gas Markets. (590/2013), Section 23(6), Section 109a of the Act on the Safety of Handling of Hazardous Chemicals and Explosives (390/2005), and the Act on Ground Stations and Certain Radars as provided for in section 8, subsection 1, paragraph 3 of the Act (96/2023).

Section 6

Jurisdiction and territoriality

This Act applies to an operator established in Finland, unless otherwise provided for by law or by European Union legislation or an international obligation binding on Finland.

Regardless of the country in which the operator is established, this Act applies to the provider of a public electronic communications network and the provider of a publicly available electronic communications service. to the provider when it offers its services in Finland.

A DNS service provider, a domain name registry administrator, a cloud service provider, a data center service provider, a content delivery network provider, a management service provider, a data security service provider, a provider of online marketplaces, a provider of online search engines and a provider of online community platforms fall within the scope of this Act if its head office referred to in Article 26(2) of the NIS 2 Directive or
The representative designated for the European Union referred to in paragraph 3 is located in Finland. If such an operator is not established in a Member State of the European Union and provides its services in Finland or in the territory of another Member State of the European Union, it must appoint a representative referred to in Article 26(3) of the NIS 2 Directive in the Member States of the European Union for the area. If the operator is not established in a Member State of the European Union or has not appointed a designated representative as referred to in Article 26(3) of the NIS 2 Directive and the operator provides services in Finland, the operator falls within the scope of this Act.

The supervisory authority may carry out supervisory or enforcement measures against an operator established in another Member State of the European Union as provided for in this Act. provided if the competent authority of another Member State requests it and the operator provides services in Finland or has a communications network or information system in the territory of Finland. A further condition is that the supervisory authority has the right to carry out the corresponding supervisory or enforcement action under this Act if the operator were established in Finland. The supervisory authority may refuse the request if it does not have the authority under the law to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks, or
the request concerns information or involves activities the disclosure or implementation of which would be contrary to the interests of Finnish national defence or national security. Before refusing the request, the supervisory authority must consult other
the relevant competent authorities and, if a Member State of the European Union so requests, requests, the European Commission and the European Union Agency for Cybersecurity.

Chapter 2

Risk management and reporting of deviations

Section 7

Risk management

The operator must identify, assess and manage risks to the security of the communication networks and information systems used in its operations or service provision. Cybersecurity risk management must prevent or minimise
the impact of incidents on operations, business continuity, service recipients and to other services.

The operator must implement risk management measures that are up-to-date, proportionate and sufficient in relation to the risks posed to the communications networks and information systems used in the operation and the importance of the communications network or information system for the operator's operations and service provision.

Section 8

Cybersecurity risk management model

The operator must have an up-to-date cybersecurity risk management model for communication networks and information systems and their physical environment. to protect against deviations and their effects.

The cybersecurity risk management framework shall identify the risks to communications networks and information systems and their physical environment, taking into account an all-hazards approach. The framework shall define and describe the cybersecurity risk management objectives, procedures

and responsibilities, as well as measures pursuant to Section 9 to protect communications networks and information systems and their physical environment is protected from cyber threats and anomalies *(control measures).*

Section 9

Measures to manage cybersecurity risks

Operators must implement proportionate technical, operational or organisational management measures in accordance with the cybersecurity risk management operating model to manage risks to the security of communications networks and information systems and to prevent or minimise harmful effects.

The operating model and the management measures based on it must take into account and must be kept up to date at least:

1) operating principles for cybersecurity risk management and assessment of the effectiveness of management measures;

2) operating principles concerning the security of communication networks and information systems;

3) the security of the acquisition, development and maintenance of communications networks and information systems, as well as the necessary procedures for handling and disclosing vulnerabilities;

4) products from direct suppliers and services from service providers in the supply chain overall quality and resilience, the management measures included in them, and the immediate cybersecurity practices of suppliers and service providers;

5) asset management and identification of functions important for its security nen;

6) personnel security and cybersecurity training;

7) access control and authentication procedures;

8) operating principles and procedures regarding the use of encryption methods and, where necessary, measures for the use of secure electronic communications;

9) observation and handling of deviations to restore safety and operational reliability for the establishment and maintenance of;

10) backup, recovery planning, crisis management and other business continuity management of security and, where necessary, the use of secure backup communication systems;

11) basic information security practices for operations, telecommunications security, hardware and to ensure software security and data security; and

12) measures to ensure the physical environment and spatial security of communication networks and information systems, as well as the necessary resources.

The measures must be proportionate to the quality and scope of the operation, the reasonably foreseeable immediate effects of the deviation, the risk exposure of the operator's communication networks and information systems, the probability and severity of the deviations, the costs arising from the measures and, taking into account current developments, the available the existing technical capabilities to counter the threat.

The supervisory authority may issue technical regulations specifying risk management obligations within its field of activity:

1) industry-specific specificities that must be taken into account in cybersecurity in the risk management operating model and in the areas referred to in subsection 2 as well as in risk management and information security management procedures for communication networks and information systems;

2) coordinated risk assessments at Union level for critical supply chains on taking results into account in industry-specific risk management.

Risk management, the risk management approach and management measures must also comply with the implementing regulations of the European Commission issued pursuant to Article 21(5) of the NIS 2 Directive.

Section 10

Management responsibility

The operator's management is responsible for implementing and maintaining cybersecurity risk management. on the organization of supervision and approves the risk management regarding cybersecurity
The operator's management must have sufficient familiarity with cybersecurity risk management.

Management refers to the operator's board of directors, supervisory board and CEO, as well as another person in a comparable position who actually directs its operations.

Section 11

Notifications of deviations to the authorities

The operator must immediately notify the supervisory authority of a significant deviation. A significant deviation means a deviation that has caused or may cause a serious disruption of services or significant financial losses.

to the relevant operator, as well as a deviation that has affected or may affect other
to natural or legal persons by causing significant material or
non-pecuniary damage.

The initial notification must be made within 24 hours of the detection of a significant deviation. and a follow-up notification within 72 hours of the detection of a significant deviation.

The initial notification must state:

1) the detection of a significant deviation;

2) whether the significant deviation is suspected to be due to a crime or other illegal act or hostile act; 3) the possibility

and likelihood of transboundary impacts and the extent of transboundary information related to impact prediction.

The follow-up notification must state:

1) an assessment of the nature, severity and impact of the significant non-conformity; 2) technical

risk indicators, if available; 3) any updates to the initial notification information.

The supervisory authority may, within its field of competence, issue more detailed technical regulations specifying the information content of the notification, information or report submitted pursuant to sections 11–15, technical form and procedure.

By way of derogation from the provisions of subsection 2 above, the trust service provider must submit a follow-up notification within 24 hours of the detection of a significant deviation if the significant deviation the deviation affects its provision of trust services.

In addition to what is referred to in subsection 1 above, a significant deviation means NIS 2 The situation in which a deviation is considered significant is specified in the European Commission implementing act adopted pursuant to Article 23(11) of the Directive.

Section 12

Interim report on the deviation

The operator must provide additional information or an interim report at the request of the supervisory authority. for status updates and progress regarding the relevant deviation.

If the significant deviation is long-lasting, the operator must submit an interim report no later than one month after submitting the follow-up notification.

Section 13

Final report on the deviation

The operator must provide the supervisory authority with a final report on a significant non-conformity within one month of submitting the follow-up notification or, in the case of a long-term non-conformity, within one month of completing its processing.

The final report must include:

1) a detailed description of the non-conformity, its severity and effects;

2) an explanation of the type of threat or root cause that likely caused the deviation;

3) a statement of the measures taken and ongoing to address the effects of the deviation to mitigate; and

4) a statement of possible transboundary impacts.

Section 14

Reporting an incident or cyber threat to someone other than the authorities

The operator must immediately notify the recipients of its services of a significant deviation if the significant deviation is likely to hinder the operator's provision of services.

The operator must immediately notify the recipients of its services who may be affected by a significant cyber threat of a significant cyber threat and of the measures available to manage the cyber threat.

If it is in the public interest to notify a significant deviation, the supervisory authority The relative can oblige the operator to inform about the matter or inform about the matter themselves.

Section 15

Voluntary reporting

Operators may voluntarily report other as well as incidents, cyber threats and near misses referred to in Section 11.

The supervisory authority must, within its field of activity, receive voluntary reports of significant deviations, incidents, cyber threats and near-misses, also from actors other than those referred to in this Act.

The supervisory authority shall provide information on notifications made under this section. to the central contact point referred to in Section 18.

Section 16

Receiving a deviation report

The supervisory authority must respond to the party that reported the non-conformity without delay. The response must include preliminary feedback on the significant non-conformity and instructions. reporting it to the criminal investigation authority if a crime is suspected in the matter.

The supervisory authority may give priority to the notifications referred to in section 11 in response to: with regard to voluntary notifications and their processing in accordance with Section 17.

Section 17

Handling of non-conformance reports

The supervisory authority shall submit the notifications and reports referred to in sections 11–13 and 15 to the CSIRT unit immediately. The CSIRT unit shall, at the request of the operator, provide instructions and operational advice on mitigation measures.

If a significant irregularity has resulted in a personal data breach referred to in Article 33 of the General Data Protection Regulation that must be reported, the supervisory authority must notify the Data Protection Commissioner of the discovery of the irregularity.

If, based on the operator's report, a significant deviation can be assumed to have been committed, the maximum penalty for which is at least three years' imprisonment, the supervisory authority must report the detection of the significant deviation to the police.

If a significant deviation has effects on other Member States of the European Union or other sectors, the supervisory authority shall inform the central contact point referred to in Section 18 thereof and submit the relevant notifications, reports and other information.

information to the contact point.

If a significant deviation affects another Member State of the European Union, the single point of contact shall notify the European Union without undue delay.

the European Cybersecurity Agency and the Member States affected by the incident. The centralised The contact point shall also, upon request, submit the notifications and reports referred to in sections 11–13 to the central contact point of the European Union Member State affected by the incident. For this purpose, the central contact point may disclose to the European Union

information about a significant incident to the European Cybersecurity Agency and the central contact points of other European Union Member States.

Section 18

Centralized point of contact

The Finnish Transport and Communications Agency's Cybersecurity Centre operates under the NIS 2 Directive. as a single point of contact referred to in Article 8(3).

The task of the central contact point is to promote cooperation between supervisory authorities. work and coordination in the implementation of tasks under this Act.

The central point of contact shall provide the European Union Agency for Cybersecurity with:

a summary report every three months containing anonymized aggregated data

Significant incidents, deviations, cyber threats and near misses reported pursuant to sections 11–13 and 15. The central point of contact shall have the right to receive for this purpose

for anonymized aggregated data from the supervisory authority.

Chapter 3

CSIRT unit

Section 19

CSIRT unit

The Finnish Transport and Communications Agency has a data breach response and investigation unit. CSIRT unit referred to in Article 1(2)(a) of the NIS 2 Directive. Its operations must be organised separately from the supervision carried out pursuant to Section 26.

The CSIRT must meet the following requirements:

1) it must ensure the full availability of its communication channels, avoiding single points of failure that completely disrupt communication, and maintain multiple means of communication by which others can contact it and it can contact others at any time;

2) its premises and the information systems supporting their operations must be located in secure places;

3) it must have an appropriate system for managing and routing requests

for, in particular, to facilitate the effective and efficient referral of cases;

4) it must ensure the confidentiality and reliability of its operations;

5) it must have sufficient staff to ensure the continuous availability of its services and must ensure appropriate training of its staff;

6) it must have contingency arrangements to ensure the continuity of its services.

The CSIRT unit must clearly define the communication channels referred to in paragraph 2, paragraph 1. channels and inform their target groups and partners about them.

Section 20

CSIRT tasks

The CSIRT unit's mission is to:

1) monitor and analyse cyber threats, vulnerabilities and incidents at the national level, collect information on them and issue early warnings, alerts, notifications and information on them;

2) assist, upon request, in real-time or near-real-time monitoring of the information security of communication networks and information systems;

3) respond to reports of incidents and, if necessary, assist the person reporting the incident party in handling the deviation;

4) collect and analyze threat intelligence and information related to the investigation of security breaches;

5) prepare risk and incident analyses and support the maintenance of the cybersecurity situational picture;

6) participate in the CSIRT network referred to in Article 15 of the NIS 2 Directive and assist its members at their request;

7) nominate experts for peer reviews referred to in Article 19 of the NIS 2 Directive; 8) promote the implementation of secure information sharing tools; 9) issue guidelines and recommendations on incident handling, cybersecurity crisis management and coordinated vulnerability disclosure.

The CSIRT unit can prioritize its tasks based on risk using according to the available resources.

The CSIRT unit coordinates the voluntary sharing arrangements for cybersecurity information referred to in section 23 between itself, the actors within the scope of this Act and other entities.

The CSIRT unit may provide a service referred to in subsection 1(2) concerning real-time or near-real-time information security monitoring of communications networks and information systems to ensure the information security of communications networks and information systems, to detect and investigate anomalies and prevent cyber threats *(information security breach detection service).* The CSIRT unit can provide information security breach detection service directly to actors and other communities that request it, as well as to information security service providers that offer information security breach detection services for use by operators or other entities *(service center).*

CSIRT unit referred to in subsection 1, paragraphs 1 and 2, and section 21, subsection 4 A fee may be charged for the service from the person requesting the service. For the services provided by the authorities on the general basis for the amount of fees charged for services and services, and Other payment criteria are laid down in the State Payment Criteria Act (150/1992).

Section 21

Web-based vulnerability assessment of public communication networks and information systems

The CSIRT unit has the right to proactively, non-intrusively, observe and map information about communication networks and information systems connected to the public communications network in order to detect vulnerabilities, cyber threats and insecurely configured communication network or information system settings *(vulnerability mapping).* Vulnerabilities

Vulnerability mapping is carried out on vulnerable or insecurely configured communication networks.
and to detect information system settings and to inform the relevant parties of the findings
to reprimand.

When carrying out a vulnerability assessment, the CSIRT unit has the right to obtain information via the public communications network about the identification data of the communications network devices, telecommunications terminals, other information systems and their telecommunications arrangements connected to it, the software used and its operation, the technical implementation and their
services provided through the vulnerability assessment. Vulnerability assessment must not cause harm to the to the operation of the targeted system or service. Vulnerability mapping should not
obtain information about communications being transmitted in a public communications network or a publicly available communications service.

Vulnerabilities detected in the vulnerability assessment and that can be linked to the subject of the assessment The information may only be used to inform the subject of the survey of vulnerabilities and risks to the communication network or information system. The CSIRT unit may use
information obtained through vulnerability assessment in addition to Section 20, subsection 1, points 1, 4 and 5 to perform the tasks for which they were intended. Unnecessary data must be deleted without delay.

The CSIRT unit has the right, at the request of the subject of the survey, to conduct a vulnerability assessment in the communications network or information systems of the subject of the survey in a manner that deviates from that provided for in subsections 1–3 in order to detect a vulnerability, cyber threat or insecurely configured settings that may have a significant impact on the communications network.
or to the information system or the services provided by them *(targeted vulnerability assessment).*

Vulnerability mapping and targeted vulnerability mapping shall not process the content of electronic messages or transmission data. The CSIRT shall destroy the information obtained in the vulnerability mapping or targeted vulnerability mapping when
they are no longer necessary for the performance of the tasks referred to in this section.

Section 22

Coordinated vulnerability disclosure

The CSIRT acts as a coordinator within the meaning of Article 12 of the NIS 2 Directive
coordinated for the disclosure of vulnerabilities. In this role, the CSIRT unit receives reports of vulnerabilities and takes care of the necessary follow-up actions resulting from them. The report may be submitted anonymously.

As a coordinator, the CSIRT unit contacts and, if necessary, acts as an intermediary between the party reporting the vulnerability and the manufacturer or provider of the ICT product or service.
between, assists those reporting vulnerabilities and negotiates the schedule for vulnerability disclosure, and coordinates the management of vulnerabilities affecting multiple actors. In addition, the CSIRT unit guides and advises on the reporting of information to the European
vulnerability database and retrieving information from it.

The CSIRT unit has the right to report information about vulnerabilities to the European Vulnerability Database:

1) which contain a description of the vulnerability;

2) the ICT products or services affected by the vulnerability, as well as the severity of the vulnerability based on the circumstances under which the vulnerability could be exploited;

3) the availability of software patches and, if they are not available, the instructions of the supervisory authority or CSIRT unit for the repair of vulnerable ICT products or services
users on how to mitigate the risks arising from the disclosed vulnerability.

If the CSIRT receives information about a vulnerability that could have a significant impact
impact on other Member States of the European Union, it must cooperate with those
with national CSIRT units in the CSIRT network.

Section 23

Voluntary cybersecurity information sharing arrangements

Voluntary arrangements for sharing cybersecurity information coordinated by the CSIRT unit, operators and other communities not covered by this Act may be established between the CSIRT unit in order to prevent and detect cyber threats to the communication networks, information systems or services of the participating communities and their customers, to manage and recover from incidents, and

to mitigate their effects.

Among those participating in a voluntary cybersecurity information sharing arrangement,
Information may be disclosed:

1) about cyber threats;
2) deviations and near misses;
3) vulnerabilities;
4) tactics, techniques and procedures; 5) indicators
of risk;
6) individual threat actors;
7) cybersecurity alerts;
8) to combat cyber threats and incidents other than those referred to in paragraphs 1–7
necessary matters.

In addition to the provisions of Section 319 of the Act on Electronic Communications Services on the disclosure of information, the CSIRT unit may disclose to a participant in a sharing arrangement information obtained while performing tasks pursuant to this Act regarding a cyber threat or incident.
related transmission information or a message containing a malicious computer program or instruction.

Notwithstanding section 136(4) of the Act on Electronic Communications Services, an operator or other entity participating in sharing arrangements may, on its own initiative, disclose to the CSIRT unit and another participant in a voluntary sharing arrangement pursuant to this Act information about transmission data related to a cyber threat or incident or about a message containing a malicious computer program or instruction.

A participant in the sharing arrangements may process information received under this section relating to a cyber threat or incident or information relating to a message containing a malicious computer program or instruction only for the purposes referred to in subsection 1.
The CSIRT may also process information received under this section for the purpose of carrying out its duties as set out in section 20(1). Disclosure of information shall not restrict the protection of confidential communications and privacy more than is necessary in accordance with subsection 1.
for the prescribed purpose.

Section 24

Data processing related to the data breach detection service

An operator using the information security breach detection service, another entity, a service center and a CSIRT unit may share with each other the information of communication networks and information systems.
information necessary for information security monitoring to prevent cyber threats and
to detect and manage incidents, recover from them and mitigate their effects. To the extent necessary to implement the data breach detection service, the information disclosed may include electronic messages
or

related transmission data that it has the right to process from electronic communications services pursuant to Section 272 of the Act.

The processing of relayed data and electronic messages in the information security breach detection service in the CSIRT unit and service center is subject to the provisions of the Electronic Communications Act.

This is provided for in sections 136–138, 145 and 272 of the Act on Cybersecurity Services. The CSIRT unit may also use the relayed information and other information it receives in connection with the provision of the service to support the maintenance of the national cybersecurity situational picture.

What is provided for in section 316, subsection 4 of the Act on Electronic Communications Services? on the destruction of information relating to the investigation of significant information security breaches or threats and on the obligation of confidentiality in section 319, subsection 1, also applies to the CSIRT unit messages and transmission data provided for the implementation of the data breach detection service.

Section 25

Information voluntarily provided to the CSIRT unit

Regardless of what is provided elsewhere in the law regarding the authorities' rights to access information, Voluntarily transferred to the CSIRT unit for the purpose of performing tasks under this Act The information may not be used in a criminal investigation against the information provider or in administrative or other proceedings against the information provider without the consent of the information provider. in decision-making.

Chapter 4

Control

Section 26

Supervisory authorities

This Act, the regulations issued pursuant to it and the regulations issued pursuant to the NIS 2 Directive Compliance with the regulations is monitored by:

1) The Finnish Transport and Communications Agency insofar as it concerns Annex I, sections 1–7 and Annex II of the operators referred to in points 1–5;

2) The Energy Authority insofar as it concerns the actors referred to in Annex I, points 8 and 9, points 10(a)–(c) and point 12(b);

3) The Finnish Safety and Chemicals Agency insofar as it concerns the operators referred to in Annex I, Section 10, points d–g, Section 11, Section 12, point a, and Annex II, Sections 6 and 11–13;

4) The Social and Health Sector Licensing and Supervision Agency insofar as it concerns the operators referred to in Annex I, section 13, subparagraphs a and b;

5) South Savo Economic Development, Transport and Environment Centre insofar as the annex is concerned the operators referred to in points 14–15 of Annex I and point 8 of Annex II;

6) The Finnish Food Authority insofar as it concerns the operators referred to in point 7 of Annex II;

7) The Finnish Medicines Agency, insofar as it concerns the provisions of Annex I, 13(c) to (f) and Annex II(9) and (10).

Supervisory authorities must cooperate in carrying out supervision.

Section 27

Targeting control

Supervision must be focused on key actors. However, the supervisory authority may also subject a non-key actor to supervision if there is a justified reason to suspect that the latter has not complied with this Act, the regulations issued pursuant to it or the provisions issued pursuant to the NIS 2 Directive.

A key actor means:

1) an operator referred to in Annex I that exceeds the conditions for medium-sized enterprises set out in Article 2 of Annex to Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises;

2) approved trust service providers, domain name registry administrators, and DNS service providers;

3) public electronic communications networks or publicly available electronic communication service providers that meet or exceed the requirements of micro, small and medium-sized enterprises Annex to Commission Recommendation 2003/361/EC concerning the definition of medium-sized enterprises the conditions for medium-sized enterprises in accordance with Article 2; and

4) an operator referred to in section 3, subsection 3.

The supervisory authority may prioritize the tasks provided for in this Act on a risk-based basis. The supervisory authority shall take into account the following in the allocation of supervision and When deciding on the use of the measures referred to in sections 29–34, the following shall be taken into account:

1) the nature and extent of the activity referred to in Annex I or II;

2) the significance of the information system or communications network for the activities referred to in Annex I or II; and 3)

the matters referred to in Section 37.

Section 28

Right to information

The supervisory authority has the right to disclose confidentiality provisions and other information. notwithstanding the restrictions on the right to obtain from the operator information on cybersecurity risk management, risk management operating model, management measures and significant deviations, as well as other information directly related to the above-mentioned information, which are necessary for monitoring compliance with the cybersecurity risk management obligation and the notification and reporting of significant deviations.

The supervisory authority has the right to disclose confidentiality provisions and other information. notwithstanding the restrictions on the right to obtain from the operator the transmission information, location information and information a message containing a malicious computer program or instruction, if necessary compliance with the cybersecurity risk management obligation or significant for the purpose of monitoring the notification and reporting of deviations. Information received by the supervisory authority pursuant to this subsection shall be kept confidential.

In the request for information, the supervisory authority must state the purpose of the request and specify the information requested. The information must be provided without delay, at the request of the authority. in the form and free of charge.

The supervisory authority has the right, notwithstanding the confidentiality provisions, the obligation of confidentiality laid down in subsection 2 and other restrictions on the disclosure of information: to hand over a document received or prepared in connection with the performance of its duties as provided for in this Act and to disclose confidential information to another supervisory authority, and to the CSIRT unit if it is necessary for the authority to perform the task provided for in this Act The exercise of the right to information or the disclosure of information may not restrict confidential message and privacy protection no more than is necessary.

The supervisory authority's right to access information does not apply to the CSIRT unit under this Act. services produced by the operator and not information.

The right to information referred to in this section does not apply to confidential information on the service production or use of the security network referred to in the Act on Public Administration Security Network Operations (10/2015), nor to information the disclosure of which would endanger national defence or national security or be contrary to them.

an important benefit related to

Section 29

Right of inspection

The supervisory authority has the right to conduct an inspection of the operator. The inspection is carried out in accordance with this Act or a regulation issued pursuant to it, or pursuant to the NIS 2 Directive. to monitor compliance with the obligations laid down in the provisions issued therein to the extent necessary.

If necessary for the quality of the inspection or for technical reasons related to it, The supervisory authority may request another supervisory authority to carry out the inspection. or use another supervisory authority, an information security assessment body and an external IT expert to assist in the inspection. The person performing the inspection and The participant must have the training and experience necessary to carry out the inspection. is necessary. The external expert is subject to criminal liability for official acts provisions concerning him when performing duties under this section. Liability for damages is provided for in the Damages Act (412/1974).

For the purpose of the inspection, operators must allow the inspector to access the communications network or information system under inspection and other premises not intended for permanent residence, to the extent required by the inspection. The inspection The supervisory authority, another authority carrying out the inspection, the information security assessment body and the external expert have the right to obtain, without prejudice to confidentiality provisions or other restrictions on the disclosure of information, to examine the information, documents, equipment and software necessary for the supervisory task, to carry out the necessary tests and measurements and to inspect the security arrangements implemented by the operator. The provisions of section 28, subsection 6, on restrictions on the right to access information shall apply to the inspector's right to inspect and access information.

The procedure to be followed in the inspection is governed by the provisions of the Administrative Procedure Act (434/2003). Section 39 provides for inspection.

Section 30

Security audit

The supervisory authority has the right to oblige the operator to commission cybersecurity a security audit focused on risk management if:

1) the operator has been subject to a significant deviation that has caused a disruption of services a malfunction of the device or significant material or immaterial damage; or

2) the operator has materially and seriously neglected to implement the cybersecurity risk management operating model referred to in section 8 or the management measures required therein, or has otherwise materially and seriously acted in breach of this Act or pursuant to it or in violation of the obligation laid down under the NIS 2 Directive.

The supervisory authority has the right to receive information about the results of the security audit and to oblige the operator to implement reasonable and proportionate measures recommended by the security audit to develop cybersecurity risk management.

Section 31

Supervision decision and warning

The supervisory authority may oblige the operator to remedy the deficiencies within a specified period of time. in the law or regulations issued pursuant to it or in regulations issued pursuant to the NIS 2 Directive in compliance with the obligations laid down in the regulations. The supervisory authority may by decision obliges the operator to disclose the deficiencies in question or other matters related to

are subject to this Act, the regulations issued pursuant to it or the NIS 2 Directive
violation of regulations.

The supervisory authority may issue a warning to the operator if he has not complied with this Act, regulations issued pursuant to it or regulations issued pursuant to the NIS 2 Directive. The warning must specify the deficiency or negligence to which it relates. The warning must be given in writing.

Section 32

Restriction of management activities

The supervisory authority may prohibit a person from acting as a key actor for a fixed period of time. as a member or deputy member of the board of directors, a member or deputy member of the supervisory board, a managing director or in another comparable position, if the latter has repeatedly and seriously violated the obligations laid down in section 10. Before making a decision, the supervisory authority must give the key actor a warning, identifying the deficiency or omission, failure to correct which may lead to a decision to restrict the activities of the management, and must set a reasonable deadline for the actor to correct the deficiency or omission. The decision may be valid for no longer than the duration of the deficiency on which it is based.

or the negligence remains uncorrected, however, for a maximum of five years.

Notwithstanding the provisions of subsection 1 above, the activities of management may not be restricted if: a private entrepreneur, a general partnership, a limited partnership, a state authority, a state enterprise, a welfare area or association, a municipal
an authority, an independent public institution, an office of Parliament, the Office of the President of the Republic, the Evangelical Lutheran Church of Finland, the Orthodox Church of Finland or their parishes, parish federations or other bodies.

Section 33

Notification to the Data Protection Commissioner

If the supervisory authority becomes aware, in connection with the performance of the tasks referred to in this Act, that a failure to comply with the obligations laid down in Chapter 2 may lead to or has led to a personal data breach referred to in the General Data Protection Regulation, of which the person referred to in the Regulation must be notified pursuant to Article 33 of the said Regulation:
to the supervisory authority, the supervisory authority must notify the Data Protection Ombudsman.

The supervisory authority must also make the notification referred to in subsection 1 to the Data Protection Ombudsman if the supervisory authority competent under the General Data Protection Regulation is located in another Member State.

Section 34

Threat of fine, threat of commission and threat of suspension

The supervisory authority may impose the following as an effect of its decision under this Act:
a threat of a fine, a threat of having the work done or a threat of suspension.

Chapter 5

Penalty fee

Section 35

Administrative penalty fee

An operator may be imposed an administrative penalty if it intentionally or negligently
Who neglects due to negligence:

1) the obligation to manage risks referred to in Section 7, the preparation of a cybersecurity risk management operating model referred to in Section 8, or the consideration of the areas referred to in Section 9, subsection 1 as part of the cybersecurity risk management operating model;

2) implement the measures referred to in section 9, subsection 2;

3) issue a deviation notification referred to in Section 11, an interim report referred to in Section 12 or the final report referred to in section 13 to the supervisory authority; 4)

provide the information referred to in section 41 to the supervisory authority.

A penalty payment cannot be imposed on state authorities, state enterprises, welfare areas or associations, municipal authorities, independent public law bodies.
institutions, parliamentary agencies, the Office of the President of the Republic, nor the Evangelical Lutheran Church of Finland and the Orthodox Church of Finland, nor their parishes, parish federations and other bodies.

Section 36

Penalty Payment Board

The Finnish Transport and Communications Agency operates a Penalty Fee Board. The board determines the administrative penalty fee based on a proposal from the supervisory authority. The administrative penalty fee is ordered to be paid to the state.

The Finnish Transport and Communications Agency appoints the chairman and vice-chairman of the board. Each supervisory authority appoints a member to the board and a personal
deputy member. The member and deputy member of the Board are required to be familiar with the management of cybersecurity risks and the NIS 2 Directive and the obligations set out in its implementing regulations within the supervisory field of the appointing authority. The Chairman and Deputy Chairman of the Board must have the necessary qualifications for the position.
sufficient legal expertise. The members of the Board are appointed for a term of three years. The Board member acts independently and impartially in his/her duties.

The decision of the Penalty Payment Board is made on the basis of a presentation. The rapporteur is an official of the supervisory authority whose supervisory jurisdiction the matter is to be resolved. The Board has a quorum when the chairman or deputy chairman is present and
at least two other members or alternate members. The decision shall be taken by the majority.
has supported. In the event of a tie, the position that is more lenient to the one
to which the sanction applies.

The Penalty Payment Board has the right, notwithstanding confidentiality provisions, to receive, free of charge, the information referred to in section 28 necessary for determining a penalty payment, as well as: other information necessary to determine the penalty or its amount
for evaluation.

Section 37

Imposing a penalty payment

The amount of the administrative penalty payment is based on an overall assessment that takes into account: taking into account the circumstances of the case and at least the following:

1) the seriousness of the violation and the importance of the provisions violated, so that the seriousness of the violation is demonstrated by

(a) the frequency of the abuses;

(b) failure to report or correct significant deviations;

c) failure to correct identified deficiencies in the decisions of the supervisory authority or despite warnings;

d) obstructing an inspection by a supervisory authority or failing to carry out a prescribed audit abandonment;

e) reporting of risk management or significant deviations to the authority in the form of false or providing misleading information;

2) the duration of the infringement;

3) any previous similar violations by the operator;

4) damage caused, including financial or economic losses, the impact on other services and the number of users affected by the breach;

5) degree of intent;

6) measures taken by the operator to prevent or mitigate the damage;

7) compliance with approved codes of conduct or approved certification mechanisms;

8) the operator's willingness to cooperate with the supervisory authority.

Section 38

Maximum penalty amount

The maximum administrative penalty imposed on a key operator is EUR 10,000,000 or two percent of the operator's global turnover for the previous financial year of the total annual turnover, whichever is greater.

The maximum amount of the administrative penalty imposed on a non-key operator is EUR 7,000,000 or 1.4 percent of the operator's total worldwide annual turnover in the preceding financial year, whichever is the greater.

Section 39

Failure to impose a penalty payment

A penalty payment will not be imposed if:

1) the operator has taken sufficient measures on its own initiative to remedy the violation or negligence immediately after its discovery and has notified the supervisory authority thereof without delay and has cooperated with the supervisory authority and the violation or negligence is not serious or repeated;

2) the violation or negligence must be considered minor; or 3) the imposition of a penalty must be considered manifestly unreasonable otherwise than on the basis referred to in paragraph 1 or 2.

A penalty payment may not be imposed if more than five years have passed since the violation or negligence has occurred. If the violation or negligence has been of a continuing nature, The deadline is calculated from the time the violation or negligence has ended.

A penalty payment may not be imposed on a person who is suspected of the same act in a preliminary investigation, in the course of criminal proceedings or in a criminal case pending in court. The penalty payment is not may also be imposed on a person who has been given a final judgment for the same act.

A penalty payment may not be imposed on a person who has been imposed a penalty payment referred to in Article 83 of the General Data Protection Regulation for the same act.

Section 40

Enforcement of penalty payment

The enforcement of the penalty payment is governed by the Act on the Enforcement of Fines. (672/2002). The penalty payment expires five years after the date of entry into force. from the date of the decision. The penalty payment expires when the natural person liable for payment dies.

Chapter 6

Other provisions

Section 41

List of actors

The supervisory authority maintains a list of operators within its supervisory field.

Operators must notify the supervisory authority of:

1) name of the operator;

2) their address, email address, telephone number and other up-to-date contact information;

3) their IP address range;

4) its relevant sector and part thereof as referred to in Annex I or II to the NIS 2 Directive; 5) whether it is a key operator; 6) a list of the Member States of the

European Union in which it provides services under the NIS 2 Directive services covered by the scope; and

7) participation in the voluntary sharing of cybersecurity information referred to in section 23.

DNS service providers, domain name registries, cloud service providers, data center service providers, content delivery network providers, management service providers, information security service providers, online marketplace providers,
Providers of online search engines and providers of online community platforms must, in addition to the information referred to in subsection 2, notify the supervisory authority of:

1) their type of operator as referred to in Annex I or II of the NIS 2 Directive;

2) its head office and other legal entities located in a Member State of the European Union the address of its premises or, if the operator is not established in the European Union, the address, email address, telephone number and other up-to-date contact details of its designated representative in the European Union; and

3) a list of the Member States of the European Union in which the operator provides services.

Operators must notify the supervisory authority of any changes to the information referred to in this section without delay. Any changes to the information referred to in subsection 2 must be notified to the supervisory authority within two weeks and any changes to the information referred to in subsection 3 within three weeks. within one month of the change. The supervisory authority may provide more detailed technical regulations on reporting information.

The supervisory authority must provide the central contact point with the NIS 2 Directive The information from the list of operators necessary for the notification referred to in Article 3(5) and Article 27(4) shall be provided. The single point of contact shall be responsible for the necessary information in the said points.

for reporting attempted breaches to the European Commission, the NIS Cooperation Group and the European Union Agency for Cybersecurity. The CSIRT unit has the right to obtain from the supervisory authority information about the list of operators from the authority.

Section 42

National Cybersecurity Strategy

The Government approves the national cybersecurity strategy and is responsible for its updating. regularly at least every five years.

The national cybersecurity strategy must include at least the NIS 2 Directive
The areas referred to in Article 7(1) and the operational principles referred to in Article 7(2).

The Government shall notify the national cybersecurity strategy to the European Commission within three months of its adoption. Information from the cybersecurity strategy may be withheld if the disclosure of such information would endanger national defence or national security or would be contrary to an important interest related to them.

Section 43

Large-scale cybersecurity incident and crisis management plan

A large-scale cybersecurity incident and crisis management plan shall be prepared to identify the capabilities, resources and procedures available in cybersecurity crisis situations. The Finnish Transport and Communications Agency is responsible for preparing the plan in cooperation with the supervisory authorities referred to in section 26,
with the police, the security police, the Defence Forces and the National Security Agency.

The plan should include measures to respond to large-scale cybersecurity incidents and crises. information necessary to manage: 1) the
objectives of national preparedness measures and actions;
2) the duties and responsibilities of the authorities;
3) crisis management practices and their inclusion in the general policy
the national crisis management framework and information exchange channels between authorities;
4) national preparedness measures, which also include exercises and training measures;

5) key public and private stakeholders and key infrastructure;
6) the procedure between authorities when participating in large-scale cybersecurity
for the coordinated management of food emergencies and crises at European Union level.

The information referred to in subsection 2 above must be notified to the European Commission and to the European Network of Cyber Crisis Contact Points referred to in Article 16 of the NIS 2 Directive within three months of the approval of the plan. Information may be withheld if its disclosure would jeopardise national defence or
national security or would be contrary to an important interest related to them.

Section 44

Cyber Crisis Management Authority

Each authority referred to in section 43(1) shall act as a cyber crisis management authority within the meaning of Article 9(1) of the NIS 2 Directive in accordance with the tasks assigned to it by law. The Cyber Security Centre of the Finnish Transport and Communications Agency shall act as
as a coordinator in the management of large-scale cybersecurity incidents and crises.

Section 45

Cooperation between authorities

Supervisory authorities, the CSIRT and the single point of contact must act
in cooperation to carry out the tasks provided for in this Act and under the NIS 2 Directive.

Supervisory authorities, the CSIRT and the single point of contact must act
if necessary, in cooperation with the police or other criminal investigation authority, the Data Protection Commissioner, The Finnish Transport and Communications Agency, in relation to the tasks provided for in the Aviation Act (864/2014), the Act on Electronic Communications Services and the eIDAS Regulation, and with the Financial Supervisory Authority.

Supervisory authorities must notify pursuant to Article 32(1) of the DORA Regulation
to the established supervisory forum when exercising their supervisory and enforcement powers over an operator designated as a third party critical ICT service provider under Article 31 of the DORA Regulation.

The supervisory authorities, the Finnish Transport and Communications Agency and the Financial Supervisory Authority, have changed
regularly exchange information on significant incidents and cyber threats.

Section 46

Appeal

The procedure for appealing to an administrative court is governed by the Administrative Procedure Act.
in the Act on Legal Affairs (808/2019).

The decision made by the supervisory authority must be complied with regardless of an appeal, unless the appeal authority determines otherwise. In an appeal, the imposition of a conditional fine and ordering payment, as well as the imposition of a threat of termination or suspension, and
However, the provisions of the UH-Cossacks Act (1113/1990) apply to the decision on the order of enforcement.

Section 47

Passage

This Act shall enter into force on 8 April 2025.

The notification referred to in section 41 of this Act must be made no later than one month after the
from the entry into force of the law or when the operator criteria in accordance with Section 3 are met.

The risk management operating model referred to in Section 8 of this Act must be prepared within three months of the entry into force of the Act or of the operator's criteria pursuant to Section 3 being met.

Helsinki, April 4, 2025

President of the Republic

Alexander Stubb

Minister of Transport and Communications Lulu Ranne

Annex I

Operators who engage in the following activities or are of the following type of operator:

1. Air traffic:

a) Common rules in the field of civil aviation security and Regulation (EC) No
Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 11 December 2002 on the
Air carriers operating on a commercial basis as defined in Article 3(4) of Regulation (EC) No 300/2008

b) Section 3, subsection 1, paragraph 2 of the Act on Airport Networks and Charges (210/2011)
airport operators referred to in

c) As defined in Article 2(1) of Regulation (EC) No 549/2004 of the European Parliament and of the
Council laying down the framework for the implementation of the single European sky
air traffic control service providers providing air traffic control service

2. Rail transport:

a) The railway network referred to in Section 4, Subsection 1, Point 29 of the Rail Traffic Act (1302/2018)
holders and companies providing traffic control services

b) Railway undertakings referred to in Section 4, Subsection 1, Point 34 of the Rail Transport Act

c) Service point operators referred to in Section 4, Subsection 1, Point 23 of the Rail Transport Act

3. Water transport:

a) Companies operating passenger and freight transport on inland waterways, seas and coastal waters
as defined in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council on
enhancing ship and port facility security, with the exception of:
excluding individual ships operated by such companies

b) Port authorities and operators referred to in section 2(2) of the Act on the Security Measures and
Supervision of Security Measures for Certain Ships and Ports Serving Them (485/2004),
who take care of the structures and equipment in the port area

c) VTS service providers referred to in section 2, subsection 1, point 5 of the Vessel Traffic Services Act
(623/2005)

4. Road traffic:

a) Road transport referred to in Chapter 15 of the Act on Transport Services (320/2017)
control and management service provider

b) Intelligent transport systems referred to in Section 160 of the Act on Transport Services
system administrators

5. In accordance with Section 2, Subsection 1, Paragraph 5 of the Act on Ground Stations and Certain Radars (96/2023),
operators referred to in this Regulation; or other entities supporting the provision of space-based services,
owned, managed and operated by Member States or private entities in the country
operators of infrastructure located in the country, with the exception of providers of public electronic
communications networks

6. Digital infrastructure:

a) Internet access points, i.e. the part of the network infrastructure that
allows more than two independent networks *(autonomous systems)*
interconnection primarily to facilitate the transmission of Internet traffic, which provides interconnection only
to autonomous systems and which does not require any Internet traffic between the two autonomous
systems it interconnects to pass through any third autonomous system, nor does it modify such traffic; or

otherwise, the administrators will interfere.

b) DNS service providers
c) Administrators of the zonal code register
d) Cloud service providers
e) Data center service providers
f) Content delivery network providers
g) Trust service providers
h) Providers of public electronic communications networks
i) Providers of publicly available electronic communications services

7. ICT service management:
a) Management service providers
b) Information security service providers

8. Electricity:

a) The electricity sector referred to in Section 3, Subsection 1, Point 21 of the Electricity Market Act (588/2013) companies that carry out electricity supply as referred to in paragraph 11
b) Distribution system operators referred to in Section 3, Subsection 1, Point 10 of the Electricity Market Act
c) Transmission system operators pursuant to Section 7 of the Electricity Market Act
d) Producers referred to in Section 3, Subsection 1, Point 15 of the Electricity Market Act
e) Regulation of the European Parliament and of the Council on the internal market in electricity Nominated electricity market operators as defined in point (8) of Article 2 of Regulation (EU) 2019/943
f) Electricity market conditions referred to in Section 3, Subsection 1, Point 37 of the Electricity Market Act parties that offer the services referred to in Section 3, Subsection 1, Point 21a of the Electricity Market Act aggregation, demand response as referred to in point 30a or energy storage as referred to in point 21c

g) Charging point operators responsible for the management and operation of a charging point providing a charging service to end users, including on behalf of a transport service provider and for

9. Operators of district heating or cooling as defined in point 19 of Directive (EU) 2018/2001 of the European Parliament and of the Council on the promotion of the use of energy from renewable sources2

10. Gas:

a) Distribution system operators referred to in section 3, subsection 1, point 10 of the Natural Gas Market Act (587/2017)
b) Transmission system operators referred to in Section 3, Subsection 1, Point 9 of the Natural Gas Market Act
c) Natural gas suppliers referred to in Section 3, Subsection 1, Point 14 of the Natural Gas Market Act

d) Storage facility holders referred to in Section 3, Subsection 1, Point 20 of the Natural Gas Market Act

e) Holders of liquefied natural gas processing equipment referred to in Section 3, Subsection 1, Point 22 of the Natural Gas Market Act
f) Natural gas companies referred to in Section 3, Subsection 1, Point 18 of the Natural Gas Market Act

g) Operators of natural gas processing and treatment facilities

11. Oil:
a) Oil pipeline operators
b) Owners of oil production, refining and processing facilities, as well as oil storage and operators handling the transfer

c) Central storage units as defined in point (f) of paragraph 2 of Council Directive 2009/119/EC on the obligation for Member States to maintain minimum stocks of crude oil and/or petroleum products

12. Hydrogen:

a) Operators engaged in hydrogen production and storage

b) Hydrogen transport operators

13. Health:

a) Section 4(2) of the Act on the Supervision of Social and Health Care (741/2023)
service providers referred to in paragraph 4 of the said section who provide the health service referred to in paragraph 4 of the said section

b) Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU
EU reference laboratories intended

c) European Medicines Agency on the Community code relating to medicinal products for human use as defined in Article 1(2) of Directive 2001/83/EC of the European Parliament and of the Council
actors involved in pharmaceutical research and development

d) Operators engaged in the manufacture of pharmaceuticals and medicinal products referred to in NACE Rev. 2, Section C, Division 21

e) Strengthening the role of the European Medicines Agency in crisis preparedness and management of the European Parliament and of the Council on medicinal products and medical devices
referred to in Article 22 of Regulation (EU) 2022/123 during a serious public health threat
Operators manufacturing medical devices considered critical (list of critical medical devices during a public health emergency)

f) Blood service establishments, pharmacies pursuant to the Blood Services Act (197/2005) and operators supplying and offering medicinal products and medical devices pursuant to Directive 2011/24/EU of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare

14. Suppliers and distributors of water intended for human consumption as defined in point (a) of Article 2(1) of Directive (EU) 2020/2184 of the European Parliament and of the Council on the quality of water intended for human consumption, with the exception of distributors for whom the distribution of water intended for human consumption is not a core part of their general activity,
which consists of the distribution of other commodities and goods

15. Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2(1), (2) and (3) of Council Directive 91/271/EEC concerning urban waste water treatment, with the exception of undertakings to which:
collection and disposal of municipal wastewater, domestic wastewater or industrial wastewater
or processing is not an essential part of their general activities

Annex II

Operators who engage in the following activities or are of the following type of operator:

1. Courier service providers and the development of the internal market for Community postal services and postal service providers referred to in Article 2(1a) of Directive 97/67/EC of the European Parliament and of the Council on common rules for the improvement of quality of service

2. Digital service providers:
a) Online marketplace providers
b) Online search engine providers
c) Online community platform providers

3. Motor vehicle driving referred to in NACE Rev. 2, Section C, Division 29
operators engaged in the manufacture of trucks, trailers and semi-trailers

4. Operators engaged in the manufacture of other transport equipment referred to in NACE Rev. 2, Section C, Division 30

5. Research organisations whose primary objective is to conduct applied research or experimental development work with a view to exploiting the results of that research for commercial purposes, but which are not higher education institutions or other educational and training institutions
institutions

6. Registration, evaluation, authorisation and restrictions of chemicals
(REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93, Commission Regulation (EC) No
1488/94, Council Directive 76/769/EEC and Commission Directives 91/155/EEC,
of the European Parliament and of the Council repealing Directives 93/67/EEC, 93/105/EC and 2000/21/EC
substances referred to in Article 3(9) of Council Regulation (EC) No 1907/2006
undertakings engaged in the manufacture and distribution of substances or mixtures referred to in point 14, as well as undertakings producing substances defined in point 3 of Article 3 of the said Regulation
articles made from substances or mixtures when the substance must be registered and the operation requires the Act on the Safety of Handling of Hazardous Chemicals and Explosives (390/2005)
A permit referred to in Section 23 or a notification referred to in Section 24

7. Regulation (EC) of the European Parliament and of the Council laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety
Food businesses as defined in Article 3(2) of Regulation (EC) No 178/2002 which carry out:
wholesale, industrial production or processing

8. Undertakings carrying out waste management as defined in point 9 of Article 3 of Directive 2008/98/EC of the European Parliament and of the Council on waste and repealing certain Directives, with the exception of undertakings for which waste management is not their main economic activity.
delinquent activity

9. On medical devices, Directive 2001/83/EC, Regulation (EC) No 178/2002 and
amending Regulation (EC) No 1223/2009 and Council Directives 90/385/EEC and
Regulation (EU) of the European Parliament and of the Council repealing Directive 93/42/EEC
Operators manufacturing medical devices as defined in Article 2(1) of Regulation (EU) 2017/745

10. On in vitro diagnostic medical devices and the Directive
Operators 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 repealing Directive 98/79/EC and Commission Decision 2010/227/EU, with the exception of operators referred to in point (e) of point 13 of Annex I to this Act

11. Computer services referred to in NACE Rev. 2, Section C, Division 26
companies engaged in the manufacture of electronic and optical products

12. Electrical equipment referred to in NACE Rev. 2, Section C, Division 27
companies engaged in the manufacture of teas

13. Other aggregates referred to in NACE Rev. 2, Section C, Division 28
Companies engaged in the manufacture of machinery and equipment

PUBLISHER: MINISTRY OF JUSTICE ISSN 1455-8904