Translation of Liechtenstein Law

Disclaimer
English is not an official language of the Principality of Liechtenstein. This translation is provided for information purposes only and has no legal force. The contents of this website have been compiled with utmost care and to the best of knowledge. However, the supplier of this website cannot assume any liability for the currency, completeness or accuracy of any of the provided pages and contents.

English title:	Cyber Security Law (CSG) of 5 December 2025
Original German title:	Cyber-Sicherheitsgesetz (CSG) vom 5. Dezember 2025
Systematic number (LR-Nr.):	784.13
First publication date:	29 January 2025
First publication no. (LGBl-Nr.):	2025-111
Last change date:	
Last change publication nr. (LGBl-Nr.):	
Translation date:	1 February 2025

Liechtenstein Law Gazette

Year 2025 No. 111 published on 29 January 2025

Cyber Security Law (CSG)

of 5 December 2025

I hereby grant My Consent to the following resolution adopted by the Liechtenstein Parliament:

I. General provisions

Art. 1

Object and scope

1) This Act lays down measures with a view to achieving a high level of cybersecurity in the public and private entities referred to in Annexes 1 and 2, which:

a) pursuant to Art. 1064 (2) or (3) of the Persons and Companies Act are considered to be medium-sized or large companies; and

b) provide their services or pursue their activities in Liechtenstein.

2) It also applies, irrespective of the size of the entity, to:

a) Entities referred to in Annexes 1 and 2, if:

1. the services are provided by:

aa) providers of public electronic communications networks or publicly accessible electronic communications services;

bb) providers of trust services;

cc) name registries of top-level domains (TLD name registries) and DNS service providers;

2. the entity is the only supplier providing a service that is indispensable for the maintenance of critical societal or economic activities;

3. a disruption of the service provided by the entity might have a significant impact on public order, public safety or public health;

4. a disruption of the service provided by the entity might lead to a significant systemic risk, in particular in sectors in which a disruption of this nature could have cross-border implications;
5. the entity is critical due to the particular importance it has at a national or regional level for the sector concerned, the specific nature of the service or for other interdependent services; or
6. the entity is an entity of State public administration;

b) Entities:

1. that have been classified as critical entities pursuant to Directive (EU) 2022/2557[1];
2. that provide domain name registration services.

3) The risk management measures and reporting obligations laid down in this Act in Art. 4 and 6 respectively, do not apply to entities of State public administration that pursue their activities in the areas of national security, public safety, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.

Art. 2

Transposition and implementation of EEA legislation

1) This Act serves to transpose and/or implement the following EEA legislation:

a) Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union[2];

b) Regulation (EU) 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres[3];

1 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333 of 27.12.2022, p. 164)

2 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for 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) (OJ L 333 of 27.12.2022, p. 80)

3 Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202 of 8.6.2021, p. 1)

c) Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification[4].

2) The current version of the EEA legislation to which this Act makes reference is to be found in the publication of the decisions of the EEA Joint Committee in the Liechtenstein Legal Gazette pursuant to Art. 3 k) of the Publications Act.

Art. 3

Definition of terms and designations

1) For the purposes of this Act the following definitions apply:

1. "network and information system" means:
   a) an electronic communications network within the meaning of Art. 3 (1) no. 5 of the Communications Act;
   b) any device or group of interconnected or related devices, one or more of which performs automatic processing of digital data on the basis of a programme; or
   c) digital data stored, processed, retrieved or transmitted by elements referred to under a) and b) for the purposes of their operation, use, protection and maintenance;
2. "security of network and information systems" means the ability of network and information systems to avert, at a given level of confidence, any event that might compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the services offered by, or accessible via, those network and information systems;
3. "cyber security" means all actions that are necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats;
4. "NIS strategy" (national cyber security strategy) means a coherent framework providing strategic objectives and priorities in the field of cyber security and the governance required for their realisation;
5. "near-miss" means any event that might have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted

4 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ. L 151 of 7.6.2019, p. 15)

or processed data or the services offered by, or accessible via, network and information systems, the occurrence of which was successfully prevented or which did not take place;

6. "security incident" means any event that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or relevant services offered by, or accessible via network and information systems;
7. "significant security incident" means a security incident, where:
   a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
   b) it has affected or is capable of adversely affecting other natural or legal persons by causing considerable material or non-material damage;
8. "large-scale cyber security incident" means a security incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States;
9. "security incident handling' means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from a security incident;
10. "risk" means the potential for loss or disruption caused by a security incident, expressed as a combination of the magnitude of such loss or disruption and the likelihood or such a security incident occurring;
11. "cyber threat" means a potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;
12. "significant cyber threat" means a cyber threat which, based on its technical characteristics, has the potential to have a severe impact on the network and information systems of an entity, or the users of such systems by causing considerable material or non-material damage;
13. "ICT product" means an element or a group of elements of a network or information system;
14. "ICT service" means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;
15. "ICT process" means any activities performed to design, develop, deliver or maintain an ICT product or ICT service;
16. "vulnerability" means a weakness, susceptibility or flaw in ICT products or ICT services that can be exploited by a cyber threat;

17. "standard" means a standard as defined in Art. 2 no. 1 of Regulation (EU) no. 1025/2012[5];
18. "technical specification" means a technical specification as defined in Art. 2 no. 4 of Regulation (EU) no. 1025/2012;
19. "internet exchange point" means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;
20. "DNS service provider" means an entity that provides:
    a) publicly available recursive domain name resolution services for internet end-users; or
    b) authoritative domain name resolution services for third-party use, with the exception of root name servers;
21. "top-level domain name registry" or "TLD name registry" means an entity which has been delegated a specific top-level domain (TLD) and is responsible for administering the TLD, including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether the operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use;
22. "entity providing domain name registration services" means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller;
23. "digital service" means a service as defined in Art. 3 (1) e) of the EEA Notifications Act;

5 Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316 of 14.11.2012, p. 12)

24. "trust service" means a trust service as defined in Art. 3 no. 16 of Regulation (EU) no. 910/2014[6];
25. "trust service provider" means a trust service provider as defined in Art. 3 no. 19 of Regulation (EU) no. 910/2014;
26. "qualified trust service" means a qualified trust service as defined in Art. 3 no. 17 of Regulation (EU) no. 910/2014;
27. "qualified trust service provider" means a qualified trust service provider as defined in Art. 3 no. 20 of Regulation (EU) no. 910/2014;
28. "online market place" means a service that allows consumers, through the use of software, including a website, a part of a website or an application operated by or on behalf of the traders, to conclude distance sales contracts with other traders or consumers;
29. "online search engine" means a digital service that allows users to input queries in the form of a keyword, voice request, group of words or other input in order to perform a search of in principle, all websites, or all websites in a particular language on any subject, and to receive results shown in any format in which information related to the requested content can be found;
30. "cloud computing service" means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;
31. "data centre service" means a service with which special structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services, together with all the facilities and infrastructures for power distribution and environmental control can be provided;
32. "content delivery network" means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;
33. "social networking services platform" means a platform that enables end-users to contact and communicate with one other and also find and share content across multiple devices, in particular via chats, posts, videos and recommendations;

6 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 (OJ L 257 of 28.8.2014, p. 73)

34. "representative" means a natural or legal person established in the EEA explicitly designated to act on behalf of a DNS service provider, an entity providing domain name registration services, a TLD name registry, a cloud computing service provider, a data centre service provider, a content delivery network operator, a managed service provider, a managed security service provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the EEA, which may be approached by a competent national authority or a CSIRT, in the place of the entity itself, with regard to the obligations of that entity under this Act;
35. "public electronic communications network" means a public electronic communications service as defined in Art. 3 (1) no. 16 of the Communications Act;
36. "electronic communications service" means an electronic communications service as defined in Art. 3 (1) no. 9 of the Communications Act;
37. "entity" means a natural person or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;
38. "managed service provider" means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely;
39. "managed security service provider" means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management;
40. "research organisation" means an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes. This does not however include educational institutions;
41. "cooperation group" means a committee established pursuant to Art. 14 of Directive (EU) 2022/2555, made up of representatives of EEA Member States, the European Commission and the European Union Agency for Network and Information Security (ENISA) and that serves to support and facilitate strategic cooperation and exchange of information between the EEA Member States in order to promote trust and confidence, with a view to achieving a high level of cybersecurity in the EEA;
42. "CSIRTs network" means a body established pursuant to Art. 15 of Directive (EU) 2022/2555, composed of representatives of the

Computer Emergency Response Teams of the EEA Member States and the IT Emergency Response Team for the bodies, institutions and other agencies of the European Union (CERT-EU) and designed to contribute to the development of confidence and trust between the EEA Member States and promote swift and effective operational cooperation;

43. "EU-CyCLONe" (European Cyber Crises Liaison Organisation Network) means a body established pursuant to Art. 16 of Directive (EU) 2022/2555, composed of the representatives of the cyber crisis management authorities of the EEA Member States and the European Commission, to provide support in the coordinated management of large-scale cyber security incidents and crises at operational level and in ensuring the regular exchange of relevant information among EEA Member States and the bodies, institutions and other agencies.

2) Under this Act the following are also considered to be:

a) essential entities:

1. entities referred to in Annex 1 which exceed the thresholds for medium-sized companies stated in Art. 1064 (2) of the Persons and Companies Act;
2. qualified trust service providers and TLD name registries, as well as DNS service providers, irrespective of their size;
3. providers of public electronic communications networks or publicly accessible electronic communications services, which are deemed to be medium-sized companies under Art. 1064 (2) of the Persons and Companies Act;
4. State public administration entities;
5. other entities listed in Annex 1 or 2 which are classified as essential entities by the Government by ordinance in accordance with the criteria of Art. 1 (2) a) nos. 2 to 6;
6. entities classified as critical entities pursuant to Directive (EU) 2022/2557;

b) important entities:

1. entities listed in Annex 1 or 2 which are not considered to be essential entities pursuant to (2);
2. other entities listed in Annex 1 or 2 which have been classified as important entities by the Government by ordinance in accordance with the criteria of Art. 1 (2) a) nos. 2 to 6.

3) The terms used in this Act to denote persons are to be understood as applying to all persons, irrespective of their gender, unless the personal terms explicitly refer to a specific gender.

II. Risk management, reporting, registration and information requirements

A. Essential and important entities

Art. 4

Risk management measure

1) Essential and important entities shall take appropriate and proportionate technical, operational and organisational measures to address the risks to the security of the network and information systems that they use for their operations or for providing their services, and to avoid or minimise the impact of security incidents on the recipients of their services and on other services.

2) Taking into account the current state of the art, and if applicable the relevant European and international standards, as well as the cost of implementation, the measures referred to under (1) shall ensure a level of security of network and information systems appropriate to the risk posed. When assessing the proportionality of these measures, the following must be duly considered:

a) the scale of the entity's exposure to risk;

b) the size of the entity; and

c) the likelihood of security incidents occurring and their severity, including their societal and economic impact.

3) The measures referred to in (1) shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from security incidents, and shall include at least the following:

a) policies on risk analysis and information system security;

b) security incident handling;

c) business continuity, such as backup management and disaster recovery, and crisis management;

d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

e) security measures in network and information systems acquisition, development and maintenance, including vulnerability management and disclosure;

f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

g) basic cyber hygiene practices and cybersecurity training;

h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

i) human resources security, access control policies and management of assets;

k) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

4) When considering which measures referred to in (3) d) are appropriate with reference to individual direct suppliers and service providers, the entity shall take into account:

a) their specific vulnerabilities;

b) the overall quality of their products;

c) their cybersecurity practices, including the security of their development processes.

5) If an entity finds that it is failing to comply with the measures provided for in (3) it shall take, without undue delay, all necessary, appropriate and proportionate corrective measures.

6) The obligations under this article do not apply if specific legislation in respect of risk management measures already exists to provide at least an equivalent level of cybersecurity.

7) The Government may establish more specific regulations concerning risk management measures by Ordinance.

Art. 5

Specific responsibilities of management bodies and authorised individuals

1) The management bodies of essential and important entities are obliged:

a) to approve the cybersecurity risk-management measures taken by those entities in order to comply with Art. 4 and oversee their implementation;

b) to participate in training and to offer appropriate training to all employees on a regular basis, to enable them to gain sufficient knowledge and skills to be able to identify and assess risks and cybersecurity management practices and their impact on the services provided by the entity.

2) Natural persons who are responsible for an essential entity or who, on the basis of their powers of representation, the authority to make decisions in the name of the entity, or their power of control over the entity, act as representative of the essential entity, must ensure that the entity complies with the provisions of this Act.

Art. 6

Reporting obligations

1) Essential and important entities shall immediately notify the National Cyber Security Unit of significant security incidents.

2) For the purposes of notification pursuant to (1) the entities concerned shall submit the following to the National Cyber Security Unit:

a) without undue delay, and in any event within 24 hours of becoming aware of the significant security incident, an early warning, which, where applicable, shall indicate whether the significant security incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

b) without undue delay, and in any event within 72 hours of becoming aware of the significant security incident, an incident notification, which, where applicable, shall update the information referred to in (a) and give an initial assessment of the significant security incident, including its severity and impact, as well as any indicators of compromise, if applicable;

c) at the request of the National Cyber Security Unit, an intermediate report on relevant status updates;

d) a final report no later than one month after the submission of the incident notification under (b), to include the following in particular:
   1. a detailed description of the security incident, including its severity and impact;
   2. information about the type of threat or root cause that is likely to have triggered the security incident;
   3. details of applied and ongoing mitigation measures;
   4. where applicable, the cross-border impact of the security incident;
e) in the event of an ongoing security incident at the time of submission of the final report referred to in (d) a progress report at the time and a final report within one month of their handling of the incident.

3) Essential and important entities shall where applicable immediately inform any recipients of their services of the significant security incident which might adversely affect the provision of the relevant services, and immediately inform them of action or mitigation measures that these recipients can take in response to this threat.

4) Notifications are to be communicated in a secure electronic format, that is standardised, as far as possible.

5) The requirements listed in (1) to (3) do not apply if specific legislation in respect of notification requirements already exists and the criteria for this reporting obligation are at least equivalent. In such cases the recipients of the notification shall report the notifications they have received immediately to the National Cyber Security Unit.

6) The Government may establish more specific regulations concerning reporting obligations of essential and important entities by Ordinance.

Art. 7

Registration requirement

1) Essential and important entities shall immediately submit the following information to the National Cyber Security Unit for the purposes of registration:

a) the name of the entity;
b) the sector, subsector and the nature of the entity on the basis of Annex 1 or 2;
c) the address of the entity's main establishment and its other legal establishments in the EEA or, if not established in the EEA, the address of its representative or authorised recipient for process;

d) up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative;

e) the EEA Member States where the entity provides services;

f) the entity's IP ranges.

2) They shall inform the National Cyber Security Unit of any changes to the information they submitted in accordance with (1) without delay and in any event within two weeks of the date of the change.

Art. 8

Informing the public

Upon receiving a notification pursuant to Art. 6 (2) b) and after consulting the entity concerned, the National Cyber Security Unit may inform the public about actual security incidents or require the entity to do so, if:

a) public awareness is necessary in order to prevent security incidents or to manage ongoing security incidents; or

b) disclosure of the security incident is otherwise in the public interest.

B. Other entities

Art. 9

Voluntary notification

1) Any entity may report security incidents, cyber threats or near-misses to the National Cyber Security Unit.

2) The voluntary notification does not have to contain the identity of the entity or information that would enable it to be identified.

Art. 10

Exchange of information

1) All entities may voluntarily exchange information on cybersecurity between themselves, including personal data, particularly in respect of:

a) cyber threats;

b) vulnerabilities;

c) tactics, technology and procedures;

d) indicators of compromise;

e) recommendations for the configuration of cybersecurity tools for detecting cyberattacks;

f) near misses.

2) The exchange of information outlined in (1) is permitted, provided that:

a) the exchange of information is intended to prevent, detect, respond to or recover from security incidents or to mitigate their impact;

b) this exchange of information enhances the level of cybersecurity, in particular by:

1. raising awareness in relation to cyber threats;
2. limiting or impeding the ability of such threats to spread;
3. supporting defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages; or
4. promoting collaborative cyber threat research between public and private entities.

IV. Organisation and Implementation

A. General

Art. 11

Responsibilities

1) The implementation of this Act is assigned to:

a) the National Cyber Security Unit;

b) the Computer Security Incident Response Team (CSIRT).

2) The National Cyber Security Unit and the CSIRT may instruct qualified third parties to perform their duties.

3) The Government may establish more specific regulations concerning the requirements for qualified third parties as referred to in (2) by Ordinance.

Art. 12

Professional confidentiality

The bodies entrusted with the implementation of this Act and any qualified third parties instructed by them shall be subject to professional confidentiality and shall maintain secrecy towards other official bodies and persons in respect of observations made in the performance of this activity and refuse access to the processed data and official files. Art. 16 is reserved.

Art. 13

Processing and disclosure of personal data

1) The National Cyber Security Unit is authorised to process personal data, including particular categories of personal data, or outsource this processing, insofar as this is necessary for the fulfilment of its duties under this Act.

2) It is authorised to divulge such data as referred to in (1), of which it becomes aware in the performance of its duties under this Act to domestic and foreign authorities and agencies, if:

a) it proves to be necessary for the performance of its duties under this Act or Directive (EU) 2022/2555;

b) confidentiality of the data is guaranteed; and

c) the security and the business interests of the essential and important entities are protected.

3) When communicating personal data to third countries or international organisations the National Cyber Security Unit shall, in addition to the requirements referred to in (2) also consider the data protection regulations set out in Chapter V of Regulation (EU) 2016/679[7] where relevant.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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) (OJ. L 119 of 4.5.2016, p. 1)

B. National Cyber Security Unit

Art. 14

Responsibilities

The National Cyber Security Unit is deemed to be:

a) the national competent authority for cybersecurity pursuant to Art. 8 (1) of Directive (EU) 2022/2555 it is responsible for the monitoring and implementation of this Act;

b) the single point of contact for cybersecurity pursuant to Art. 8 (3) of Directive (EU) 2022/2555; it also exercises a liaison function to ensure cross-border cooperation with international bodies and groups, such as, in particular, the competent bodies in other EEA Member States, the cooperation group and the CSIRTs network;

c) the competent authority for the management of large-scale cybersecurity incidents and crises pursuant to Art. 9 (1) of Directive (EU) 2022/2555;

d) the competent authority for cybersecurity certification pursuant to Art. 58 (1) of Regulation (EU) 2019/881; it performs the duties and exercises the powers referred to in Art. 58 (7) and (8) of the aforementioned Regulation.

Art. 15

Duties

1) The National Cyber Security Unit shall adopt the measures required within the context of its mandate to ensure compliance with this Act. It is responsible, in particular for:

a) verification of the risk management measures set out in Art. 4 and compliance with the reporting obligations set out in Art. 6;

b) establishment and coordination of the CSIRT pursuant to Art. 20;

c) receipt and analysis of notifications of risks or security incidents, drawing up a survey of the situation and forwarding the notifications and the survey of the situation, together with additional relevant information to the domestic authorities or other concerned bodies, where required;

d) drawing up and disclosure of relevant information to guarantee cybersecurity or for the prevention of security incidents;

e) keeping a register containing data on the essential and important entities and entities that provide domain name registration services, as well as performing a regular review and update of the register contents, at least once every two years;

f) receipt of nominations and keeping of a list of representatives pursuant to Art. 3 (1) no. 34;

g) promotion of the use of European and international standards and technical specifications for the security of network and information systems;

h) notification and forwarding of information provided by essential and important entities to the single point of contact of the EEA Member States concerned, if a security incident has cross-border implications for those EEA Member States;

i) coordination and promotion of public-private cooperation in cybersecurity matters;

k) informing the public of security incidents, raising public awareness in order to prevent or manage security incidents and publishing general information in connection with cybersecurity;

l) cooperation and exchange of information with other domestic authorities and bodies, in particular the National Police Force, the Public Prosecution Service, the Data Protection Office, the Office for Information Technology, the Office for Communications, the Office for Civil Protection, the Office of Building Construction and Spatial Planning, the Civil Engineering and Geoinformation Office, the Financial Intelligence Unit and the Liechtenstein Financial Market Authority;

m) cooperation with the National Emergency Management Staff and coordination of the work to develop a national plan for the response to large-scale cybersecurity incidents and crises;

n) cross-border cooperation and cross-border exchange of information, in particular in the case of mutual assistance or a significant security incident or a large-scale cybersecurity incident affecting two or more EEA Member States, with the competent authorities and agencies in other EEA Member States, ENISA, the cooperation group, EU-CyCLONe and the CSIRTs network;

o) cross-border cooperation and cross-border exchange of information in relation to cybersecurity with the competent authorities and agencies in third countries;

p) coordination of the establishment of an NIS strategy pursuant to Art. 21;

q) representing Liechtenstein in the cooperation group, the CSIRTs network, EU-CyCLONe, the European Cybersecurity Certification Group and in other cross-border organisations in the EEA and international bodies for cybersecurity;

r) participation in peer reviews pursuant to Art. 19 of Directive (EU) 2022/2555.

2) The National Cyber Security Unit may, after consulting the appropriate member of the Government, conclude agreements with other domestic and foreign authorities concerning the cooperation arrangements and cooperate with private individuals under public-private partnerships for the performance of its duties.

3) The Government may establish more specific regulations concerning the duties of the National Cyber Security Unit by Ordinance.

Art. 16

Powers with regard to essential and important entities

1) In the performance of its duties under this Act, the National Cyber Security Unit may require essential and important entities to:

a) provide it with the information necessary to assess cybersecurity, including the risk management measures taken, as well as the documented cybersecurity policies;

b) provide it with evidence of the effective implementation of cybersecurity policies;

c) disclose information free of charge, in particular, technical and statistical data, for statistical purposes or the creation of physical surveys of the situation.

2) It may furthermore oblige essential or important entities to:

a) inform the natural or legal persons for whom they provide services or carry out activities and who are potentially affected by a significant cyber threat, of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;

b) where justified, designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with the risk management measures and reporting obligations laid down in Art. 4 and 6;

c) use special ICT products, services and processes that are certified under European cybersecurity certification schemes adopted pursuant

to Art. 49 of Regulation (EU) 2019/881, in order to meet specific requirements pursuant to Art. 4.

3) It is authorised to conduct security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned.

4) Essential and important entities may not refuse to disclose the information referred to in (1) c) on grounds of professional, commercial or industrial confidentiality.

Art. 17

Powers in the event of infringements

1) If the National Cyber Security Unit has evidence that an essential or important entity is in breach of the provisions of this Act, the ordinances enacted in connection with them, or decisions or orders based on them, it shall informally notify the essential or important entity of this, subject to (5), and set it an appropriate deadline to:

a) comment on the notification; or

b) restore the situation to a lawful state of affairs.

2) The National Cyber Security Unit may extend the deadline referred to in (1) b) in justified cases on request, if the essential or important entity can there-by be expected to restore the situation to the lawful state of affairs.

3) If the essential or important entity is a public-sector body or an entity that is charged with public functions, the National Cyber Security Unit shall also inform the Government about the notice referred to in (1).

4) If there are indications of infringements against the provisions of this Act or ordinances enacted in connection with them by essential or important entities, the National Cyber Security Unit shall inform the competent supervisory authority and give them the opportunity to comment before a notice as referred to in (1) is issued.

5) If an essential or important entity fails to comply with the notice referred to in (1) the National Cyber Security Unit shall issue an appropriate order on the matter; in urgent cases an order may be issued without a notice. The National Cyber Security Unit shall inform the competent supervisory authority for the essential or important entity of the decision.

6) The imposition of fines pursuant to Art. 23 is reserved.

Art. 18

Use of information and communications technology solutions (ICT solutions)

In order to perform its duties, the National Cyber Security Unit is authorised to:

a) employ ICT solutions or instruct third parties to employ them, in order to identify the risks or security incidents arising in network and information systems in good time;

b) employ ICT solutions, or use them after obtaining the consent of the entity concerned, in order to identify the patterns of attacks on network and information systems;

c) employ ICT solutions to conduct security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria;

d) employ ICT solutions or instruct third parties to employ them, to conduct Internet searches and in this connection also to register on and log into forums or websites available to a restricted group of users and subsequently download and analyse data, including personal data from the Internet.

Art. 19

Control measures

1) The National Cyber Security Unit may carry out control measures to check compliance with the requirements pursuant to this Act or instruct qualified third parties to perform this function.

2) In order to carry out control measures the National Cyber Security Unit, or the qualified third parties it has instructed, may inspect the network and information systems used by essential and important entities and the relevant records. To complete their inspection, they have the right to enter premises in which network and information systems are located. The inspection must be conducted proportionately and with the highest possible level of protection for the rights of the entity and third parties concerned and for the business.

3) The Government may establish more specific regulations concerning the performance of control measures by Ordinance.

C. Computer security incident response team (CSIRT)

Art. 20

Purpose and responsibilities

1) In order to guarantee cybersecurity a CSIRT shall be established at the National Cyber Security Unit. It is responsible, in particular, for:

a) provision of information that may be useful for dealing with a security incident or guidance for the implementation of possible mitigation measures on receipt of notifications of risks or security incidents as referred to in Art. 6 and 9;

b) issuing early warnings and alerts, as well as announcement and dissemination of information to relevant stakeholders about cyber threats, vulnerabilities and security incidents;

c) the initial general or technical assistance in responding to a security incident;

d) providing assistance to essential and important entities as regards monitoring of their network and information systems, on request;

e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact or proactive non-intrusive scanning of publicly accessible network and information systems on their own initiative (vulnerability scan);

f) observation and analysis, including analysis of forensic data and dynamic analysis of risks, cyber threats, vulnerabilities and security incidents, as well as situational awareness;

g) cooperation with sectoral or cross-sectoral communities of essential and important entities and exchanging relevant information;

h) promoting the use of common or standardised practices, classification schemes and taxonomies in relation to incident-handling procedures, crisis management and coordinated vulnerability disclosure;

i) participating in the CSIRTs network;

k) cooperation with national computer security incident response teams or equivalent third-country bodies, in particular for the purpose of providing them with cybersecurity assistance.

2) The CSIRT may also perform the duties listed in (1) a) to c) and f) with respect to other entities or individuals, if they are affected by a risk or a security incident in their network and information systems.

3) It acts as a coordinator and trusted intermediary for the purposes of coordinated vulnerability disclosure pursuant to Art. 12 (1) of Directive (EU) 2022/2555.

4) The Government may establish more specific regulations concerning the purpose and responsibilities of the CSIRT by Ordinance.

D. NIS strategy

Art. 21

Basic principle

1) The NIS strategy shall define in particular the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity.

2) The NIS strategy shall be regularly assessed, at least every five years, on the basis of key performance indicators and updated if necessary.

3) The NIS strategy must be approved by the Government and once approved will be published on the National Cyber Security Unit website.

IV. Legal remedy

Art. 22

Appeal

1) Appeals may be lodged with the Board of Appeal for Administrative Matters against decisions and orders of the National Cyber Security Unit within 14 days from notification.

2) Appeals may be lodged with the Administrative Court against decisions and orders of the Board of Appeal for Administrative Matters within 14 days from notification.

3) The powers of review of the Board of Appeal for Administrative Matters and the Administrative Court are restricted to legal and substantive issues. The exercise of discretion is examined purely in a legal context.

4) In other respects, the proceedings will be subject to the provisions of the General National Administration Act.

V. Penal provisions

Art. 23

Infringements

1) Provided the offence in question does not constitute a criminal offence falling within the jurisdiction of the courts, the National Cyber Security Unit shall impose fines pursuant to (2) for an offence, on any person who:

a) fails to take the risk management measures prescribed in Art. 4;

b) fails to comply with the reporting obligations laid down in Art. 6;

c) fails to comply with the registration requirements laid down in Art. 7 (1);

d) fails to inform the National Cyber Security Unit of changes within the period stipulated pursuant to Art. 7 (2);

e) fails to provide the information required under Art. 16 (1) a), including documented security measures;

f) fails to provide evidence pursuant to Art. 16 (1) b);

g) fails to disclose information referred to in Art. 16 (1) c) to the National Cyber Security Unit;

h) fails to comply with the obligation laid down in Art. 16 (2) a);

i) fails to comply with the obligation to appoint a monitoring officer as referred to in Art. 16 (2) b);

k) fails to comply with the obligation to use special ICT products, services and processes pursuant to Art. 16 (2) c);

l) impedes, obstructs or renders impossible the proper performance of a control measure pursuant to Art. 19;

m) contravenes a legally binding order or decision of the National Cyber Security Unit.

2) The fines imposed pursuant to (1):

a) shall for essential entities be set at up to 10 000 000 Francs, or up to 2 % of the total global turnover achieved in the previous financial year by the company to which the essential entity belongs, whichever amount is higher;

b) shall for important entities be set at up to 7 000 000 Francs, or up to 1.4 % of the total global turnover achieved in the previous financial year by the company to which the essential entity belongs, whichever amount is higher.

3) Provided the offence in question does not constitute a criminal offence falling within the jurisdiction of the courts, the National Cyber Security Unit shall impose fines of up to 100 000 Francs for an offence, on any person who contravenes Regulation (EU) 2019/881, if they:

a) as a manufacturer or supplier of ICT products, services and processes fail to comply with the obligations under Art. 53 (2) or (3);

b) as a manufacturer or supplier of certified ICT products, services or processes or ICT products, services and processes fail to meet the requirements of Art. 55;

c) as a conformity assessment body as referred to in Art. 60 fail to issue a European cybersecurity certificate in the proper manner pursuant to Art. 56 (4);

d) as a holder of a European cybersecurity certificate fail to meet the obligations referred to in Art. 56 (8); or

e) as a manufacturer or supplier of ICT products, services or processes, who carries out a self-assessment of conformity, or as a conformity assessment body as referred to in Art. 60 impede, obstruct or render impossible the monitoring and supervision of the provisions of Regulation (EU) 2019/881 by the National Cyber Security Unit.

4) When imposing a fine pursuant to (1) to (3) the National Cyber Security Unit shall take into account:

a) the seriousness of the infringement and the importance of the provisions breached, whereby the following are to be considered as a serious infringement in all cases:
   1. repeated offences;
   2. a failure to notify or remedy significant security incidents;
   3. a failure to remedy deficiencies following binding instructions from the National Cyber Security Unit pursuant to Art. 17 (5);
   4. the obstruction of control measures referred to in Art. 19, that are carried out following detection of an infringement by the National Cyber Security Unit or by qualified third parties it has instructed;
   5. providing false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting obligations laid down in Art. 4 and 6;

b) the duration of the infringement;

c) any relevant previous infringements on the part of the entity concerned;

d) any material or non-material damage caused, including any financial or economic loss, effects on other services and the number of users affected;

e) any measures taken by the entity to prevent or mitigate the material or non-material damage;

f) adherence to approved codes of conduct or approved certification mechanisms;

g) the level of cooperation of the natural or legal persons held responsible with the competent authorities.

5) In the event of negligence, the upper limit of the penalty stated in (2) and (3) is reduced by half.

6) No fines are imposed against State public administration institutions.

Art. 24

Liability

If criminal offences are committed in the course of business of a legal entity, a partnership or a sole trader, the penal provisions shall apply to those persons who acted, or should have acted on their behalf, but subject to the joint and several liability of the legal entity, the partnership or the sole trader for the fines and costs.

VI. Transitional and final provisions

Art. 25

Implementing Regulations

The Government shall enact the Ordinances required for the implementation of this Act.

Art. 26

Transitional provision

Essential and important entities existing at the time when this Act comes into force must submit the information listed in Art. 7 (1) to the National Cyber Security Unit for the purposes of registration within four weeks from the entry into force of this Act.

Art. 27

Repeal of the previous Act

The Cyber Security Act (CSG) of 4 May 2023, Liechtenstein Legal Gazette (LGBl.) 2023 no. 269, is repealed.

Art. 28

Applicability of EU legislation

1) Until they are adopted into the EEA Agreement the following shall apply as national legislation:

a) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for 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);

b) the implementing acts in respect of Directive (EU) 2022/2555.

2) The full text of the legislation referred to in (1) is published in the Official Journal of the European Union at *https://eur-lex.europa.eu*; it can be viewed on the National Cyber Security Unit website at *https://scs.llv.li*.

Art. 29

Entry into force

1) Provided that the referendum deadline expires unutilised, this Act shall enter into force on 1 February 2025, otherwise on the day after promulgation.

2) Art. 2 (1) a) shall enter into force at the same time as the Decision of the EEA Joint Committee concerning the adoption of Directive (EU) 2022/2555 in the EEA Agreement.

In representation of the Prince Regnant:
sig. *Alois*
Hereditary Prince

sig. *Daniel Risch*
Prime Minister of the
Principality of Liechtenstein

Annex 1
(Art. 1, 3 and 7)

Sectors of high criticality

Sector	Subsector	Type of entity
1. Energy	a) Electricity	– Electricity undertakings as defined in Art. 3 (1) no. 34, Electricity Market Act, which perform the function of 'supply' as defined in Art. 3 (1) no. 20 of the said Act – Distribution system operators as defined in Art. 3 (1) no. 19, Electricity Market Act – Transmission system operators as defined in Art. 3 (1) no. 18, Electricity Market Act – Producers as defined in Art. 3 (1) no. 2, Electricity Market Act – Nominated electricity market operators as defined in Art. 2 no. 8 of Regulation (EU) 2019/943[8] – Market participants as defined in Art. 2 no. 25 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2 nos. 18, 20 and 59 of Directive (EU) 2019/944[9] – Operators of recharging points that are responsible for the management and operation of a recharging point, which provide a recharging service to end users, including in the name and on behalf of a

8 Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158 of 14.6.2019, p. 54)
9 Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158 of 14.6.2019, p. 125)

		mobility service provider
	b) District heating and cooling	– Operators of district heating or district cooling as defined in Art. 2 no. 19 of Directive (EU) 2018/2001[10]
	c) Oil	– Operators of oil transmission pipelines – Operators of oil production, refining and treatment facilities, storage and transmission – Central stockholding entities as defined in Art. 2 f) Directive 2009/119/EC[11]
	d) Gas	– Supply undertakings as defined in Art. 4 (1) no. 10 Gas Market Act – Distribution system operators as defined in Art. 4 (1) no. 8 Gas Market Act – Transmission system operators as defined in Art. 4 (1) no. 6 Gas Market Act – Storage system operators as defined in Art. 4 (1) no. 12 Gas Market Act – LNG system operators as defined in Art. 4 (1) no. 14 Gas Market Act – Natural gas undertakings as defined in Art. 4 (1) no. 4 Gas Market Act – Operators of natural gas refining and treatment facilities
	e) Hydrogen	– Operators of hydrogen production, storage and transmission

10 Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328 of 21.12.2018, p. 82)

11 Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265 of 9.10.2009, p. 9)

2. Transport	a) Air	– Air carriers as defined in Art. 3 no. 4 Regulation (EC) no. 300/2008[12], used for commercial purposes – Airport managing bodies as defined in Art. 2 no. 2 of Directive 2009/12/EG[13], airports as defined in Art. 2 no. 1 of that Directive, including the core airports listed in Annex II of Regulation (EU) 2024/1679[14], and entities operating ancillary installations contained within airports – Traffic management control operators providing air traffic control (ATC) services as defined in Art. 2 no. 1 of Regulation (EC) no. 549/2004[15]
	b) Rail	– Infrastructure managers as defined in Art. 3 (1) b) Railways Act – Railway undertakings as defined in Art. 3 (1) a) Railways Act, including operators of service facilities as defined in Art. 3 no. 12 of Directive 2012/34/EU[16]

12 Regulation (EC) no. 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ. L 97 of 9.4.2008, p. 72)

13 Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges OJ L 70 of 14.3.2009, p. 11)

14 Regulation (EU) 2024/1679 of the European Parliament and of the Council of 13 June 2024 on Union guidelines for the development of the trans-European transport network, amending Regulations (EU) 2021/1153 and (EU) no 913/2010 and repealing Regulation (EU) no 1315/2013 (OJ L 2024/1679 of 28.6.2024)

15 Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) - Statement by the Member States on military issues related to the single European sky (OJ L 96 of 31.3.2004, p. 1)

16 Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343 of 14.12.2012, p. 32)

	c) Water	– Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) no. 725/2004[17], not including the individual vessels operated by those companies – Managing bodies of ports as defined in Art. 3 no. 1 of Directive 2005/65/EC[18], including their port facilities as defined in Art. 2 no. 11 of Regulation (EC) no. 725/2004, and entities operating works and equipment contained within ports – Operators of vessel traffic services (VTS) as defined in Art. 3 o) of Directive 2002/59/EC[19]
	d) Road	– Road authorities as defined in Art. 2 no. 12 of Delegated Regulation (EU) 2015/962[20], responsible for traffic management control, excluding 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 as defined in Art. 4 no. 1 of Directive 2010/40/EU[21]

17 Regulation (EC) no. 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129 of 29.4.2004, p. 6)

18 Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310 of 25.11.2005, p. 28)

19 Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208 of 5.8.2002, p. 10)

20 Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157 of 23.6.2015, p. 21)

21 Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207 of 6.8.2010, p. 1)

3. Banking		Credit institutions as defined in Art. 4 no. 1 of Regulation (EU) no. 575/2013[22]
4. Financial market infrastructures		– Operators of trading venues as defined in Art. 3 (1) no. 1 of the Trading Venue and Stock Exchange Act – Central counterparties (CCPs) as defined in Art. 2 no. 1 Regulation (EU) Nr. 648/2012[23]
5. Health		– Healthcare providers as defined in Art. 3 g) of Directive 2011/24/EU[24] – EU reference laboratories as defined in Art. 15 of Regulation (EU) 2022/2371[25] – Entities carrying out research and development activities in medicinal products as defined in Art. 4 (1) a) of the EEA Medicinal Products Act – Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 – Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list) within the meaning of Art. 22 of Regulation (EU) 2022/123[26]

22 Regulation (EU) no. 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 646/2012 (OJ L 176 of 27.6.2013, p. 1)

23 Regulation (EU) no. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201 of 27.7.2012, p. 1)

24 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88 of 4.4.2011, p. 45)

25 Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314 of 6.12.2022, p. 26)

26 Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20 of 31.1.2022, p. 1)

6. Drinking water		Suppliers and distributors of "water intended for human consumption" as defined in Art. 2 no.1 a) of Directive (EU) 2020/2184[27], but excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods
7. Waste water		Undertakings collecting, disposing of or treating waste water pursuant to Art. 5 (1) h) Water Protection Act, but excluding undertakings for which collecting, disposing of or treating such waste water is a non-essential part of their general activity
8. Digital infrastructure		– Internet exchange point providers – DNS service providers, excluding operators of root name servers – TLD name registries – Cloud computing service providers – Data centre service providers – Content delivery network operators – Trust service providers – Providers of public electronic communications networks or – Providers of publicly available electronic communications services
9. ICT service management (business-to-business)		– Managed service providers – Managed security service providers
10. Public administration		State public administration entities

27 Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (OJ L 435 of 23.12.2020, p. 1)

11. Space		Operators of ground-based infrastructure, owned, managed and operated by the Principality of Liechtenstein or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

Annex 2

(Art. 1, 3 and 7)

Other critical sectors

Sector	Subsector	Type of entity
1. Postal and courier services		Postal service providers as defined in Art. 3 (1) k) Postal Services and Parcel Delivery Services Act, including providers of courier services
2. Waste management		Undertakings carrying out waste management as defined in Art. 3 no. 9 of Directive 2008/98/EC[28], excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		Undertakings engaged in the manufacture of substances and in trade in substances or mixtures, as referred to in Art. 3 nos. 9 and 14 Regulation (EC) no. 1907/2006[29], and undertakings carrying out the production of articles, as defined in Article 3, no. 3 of that Regulation, from substances or mixtures

28 Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312 of 22.11.2008, p. 3)

29 Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396 of 30.12.2006, p. 1)

4. Production, processing and distribution of food		Food businesses as defined in Art. 3 no. 2 Regulation (EC) no. 178/2002[30], which are 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 Art. 2 no. 1 Regulation (EU) 2017/745[31], and entities manufacturing in vitro diagnostic medical devices as defined in Art. 2 no. 2 Regulation (EU) 2017/746[32], with the exception of entities manufacturing medical devices referred to in Annex I, no. 5, fifth indent, of this Directive
	b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
	d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2

30 Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 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 (OJ L 31 of 1.2.2002, p. 1)

31 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117 of 5.5.2017, p. 1)

32 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117 of 5.5.2017, p. 176)

	e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
	f) Manufacture of other transport equipment	Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2
6. Digital providers		– Providers of online market places – Providers of online search engines – Providers of social networking services platforms
7. Research		Research organisations