EnCaViBS

WP 2: The NIS Directive and its transposition into national law.

Member State:
Luxembourg

Act of 28 May 2019 transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a common high level of network and information system security in the European Union and amending

1° the amended Act of 20 April 2009 establishing the State Information Technology Centre and

2° the Act of 23 July 2016 establishing a High Commission for National Protection.

Important notice:

This text is an unofficial translation conducted at the SnT/ University of Luxembourg in the framework of the research project EnCaViBS.

The original legal acts which Member States notified to the European Commission as national execution measures were retrieved from official national databases. In order to focus on the core of the research project, only selected transpositions have been translated.

The translations only serve the purpose of being an information resource; there is no guarantee whatsoever that the translations correctly correspond to the original versions of the laws. Therefore, evidently, the texts have no legal value. The original, as well as the translated version of the legal acts, are available at www.encavibs.uni.lu, where additional information on the research project may be found.

This research project is funded by the Luxembourg National Research Fund (FNR), C18/IS/12639666/EnCaViBS/Cole,

https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

Fonds National de la Recherche Luxembourg

Member State: Luxembourg

Act of 28 May 2019 transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a common high level of network and information system security in the European Union and amending

3° the amended Act of 20 April 2009 establishing the State Information Technology Centre and

4° the Act of 23 July 2016 establishing a High Commission for National Protection.

Official Journal of the Grand Duchy of Luxembourg, Mémorial A no 372 of 31 May 2019

We Henri, Grand Duke of Luxembourg, Duke of Nassau,
Our Council of State heard;

With the assent of the Chamber of Deputies;

Having regard to the decision of the Chamber of Deputies of 15 May 2019 and the decision of the Council of State of 21 May 2019 that there is no need for a second vote;

Have ordered and do order:

Chapter 1 - Definitions and Scope

Art. 1.

(1) The security and notification requirements provided for in this Act shall not apply to undertakings subject to the requirements set out in Articles 45 and 46 of the amended Act of 27 February 2011 on electronic communications networks and services or to trust service providers subject to the requirements in Article 19 of 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.

(2) Where a Union law or sectoral legal act requires operators of essential services or digital service providers to ensure the security of their networks and information systems or to carry out incident reporting, provided that the requirements in question are at least equivalent in effect to the obligations laid down in this Act, the provisions of that Union law or sectoral legal act shall apply.

Art. 2.

For the purposes of this Act, the following definitions apply

1° "Network and Information System":

a) an electronic communications network within the meaning of Article 2(24) of the amended Act of 27 February 2011 on electronic communications networks and services;

b) any device or set of interconnected or related devices, one or more of which, in execution of a program, performs automated processing of digital data; or

c) digital data stored, processed, retrieved or transmitted by the elements referred to in subparagraphs (a) and (b) for the purpose of their operation, use, protection and maintenance;

2° "Security of networks and information systems" means the ability of networks and information systems to withstand, at a given level of confidence, actions that compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data and the related services that these networks and information systems provide or make available;

3° "Operator of essential services" means a public or private entity of the type listed in the Annex which meets the criteria set out in Article 7(2);

4° "Digital service" means a service within the meaning of Article 1(1)(b) of the Act of 8 November 2016 providing for an information procedure in the field of technical regulations and rules on information society services of the type "online marketplace", "online search engine" or "cloud computing service";

5° "Digital Service Provider" means a legal entity that provides a digital service;

6° "Incident" means any event that has an actual negative impact on the security of networks and information systems;

7° "Incident Management" means all procedures useful for the detection, analysis and containment of an incident and all procedures useful for the response to an incident;

8° "Risk" means any reasonably identifiable circumstance or event that has a potential adverse impact on the security of networks and information systems;

9° "Representative" means a natural or legal person established in the European Union who is specifically appointed to act on behalf of a digital service provider not established in the European Union;

10° "Standard" means a standard within the meaning of Article 2(1) of 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;

11° "Specification": a technical specification within the meaning of Article 2(4) of 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;

12° "Internet Exchange Point", hereinafter "IXP", means a network structure that permits the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of Internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require Internet traffic passing between any pair of participating autonomous systems to transit through a third autonomous system, nor does it otherwise modify or alter such traffic;

13° "Domain Name System", hereinafter "DNS", means a hierarchical and distributed system of assigning names in a network that resolves domain name issues;

14° "DNS Service Provider" means an entity that provides DNS services on the Internet;

15° "Top Level Domain Registry" means an entity that administers and manages the registration of Internet domain names in a given Top Level Domain;

16° "Online marketplace" means a digital service that allows consumers or professionals within the meaning of Article L. 010-1, point 1 or point 2 respectively, of the Consumer Code to conclude online sales or service contracts with traders either on the website of the online marketplace or on the website of a trader who uses the IT services provided by the online marketplace;

17° "Online search engine" means a digital service that allows users to search, in principle, all websites or websites in a given language, on the basis of a query on any subject in the form of a keyword, phrase or other entry, and which returns links from which information related to the requested content can be found;

18° "Cloud computing service" means a digital service that provides access to a scalable and variable set of computing resources that can be shared;

19° "Government CERT": Computer Emergency Processing Centre, as defined in the Grand-Ducal Decree of 9 May 2018 determining the organisation and powers of the Computer Emergency Processing Centre, known as the "Government CERT";

20° "CIRCL": Computer Incident Response Center Luxembourg, operated by the economic interest grouping Security Made in Lëtzebuerg;

21° "CSIRT": Computer Security Incident Response Center;

22° "Cooperation Group" means a group established to support and facilitate strategic cooperation and information exchange between Member States and to build confidence and achieve a common high level of security of networks and information systems in the European Union;

23° "CSIRT Network": a group established to contribute to confidence-building among Member States and to promote rapid and effective operational cooperation;

24° "Single National Contact Point" means an authority which acts as a liaison to ensure cross-border cooperation between Member States' authorities, as well as with the relevant authorities of other Member States, the Cooperation Group and the CSIRT network.

Chapter 2 - Relevant competent authorities and single national contact point

Art. 3.

The Commission de surveillance du secteur financier, hereinafter "the CSSF", is the competent authority for the security of networks and information systems covering the sectors of credit institutions and financial market infrastructures as defined in points 3 and 4 of the Annex, as well as the digital services provided by an entity falling under the supervision of the CSSF.

The Institut luxembourgeois de régulation, hereinafter "ILR", is the competent authority for the security of networks and information systems covering the other sectors referred to in the Annex, as well as digital services provided by an entity for which the CSSF is not the competent authority.

The obligation of professional secrecy provided for in Article 16 of the amended law of 23 December 1998 creating a Financial Sector Supervisory Commission and in Article 15 of the amended law of 30 May 2005 on: 1) organisation of the Institut Luxembourgeois de Régulation; 2) amendment of the amended Law of 22 June 1963 laying down the salary system for State officials does not preclude the exchange of information between competent authorities.

Art. 4.

The ILR is the single national point of contact for network and information system security.

Art. 5.

The ILR shall receive a financial contribution from the State budget to cover all the operating costs arising from the performance of the tasks provided for in this Law.

Art. 6.

To the extent necessary for the performance of their tasks under this Law, the competent authorities and the single national contact point shall consult and cooperate with the competent national law enforcement authorities and the national data protection authorities.

The obligation of professional secrecy provided for in Article 16 of the amended law of 23 December 1998 creating a Financial Sector Supervisory Commission and in Article 15 of the amended law of 30 May 2005

on: 1) organisation of the Institut Luxembourgeois de Régulation; 2) amendment of the amended law of 22 June 1963 fixing the salary system for State officials does not preclude such cooperation.

Chapter 3 - Operators of essential services

Art. 7.

(1) Operators of essential services with an establishment on Luxembourg territory fall within the scope of this law.

(2) The identification of operators of essential services by the relevant competent authority shall be carried out using the following identification criteria:

1° the entity provides a service that is essential to the maintenance of critical societal and/or economic activities;

2° the provision of this service is dependent on networks and information systems; and

3° an incident would have a significant disruptive effect on the provision of that service.

The competent authority concerned shall notify the identification decision to the operator of essential services.

(3) The significance of the disruptive effect referred to in paragraph 2(3) shall be determined on the basis of cross-sectoral and sectoral factors, including at least:

1° the number of users dependent on the service provided by the entity concerned;

2° the dependence of other Annex I sectors on the service provided by that entity;

3° the consequences that incidents could have, in terms of degree and duration, on economic or societal functions or on public safety;

4° the market share of this entity;

5° geographical scope in terms of the area likely to be affected by an incident;

6° the importance of the entity in ensuring an adequate level of service, taking into account the availability of alternatives for the provision of that service.

(4) The list of essential services shall be determined by the competent authority concerned by means of a regulation.

(5) Where an entity provides a service referred to in point 1 of paragraph 2 in another Member State, the competent authority concerned shall consult the competent authority of the other Member State. The consultation takes place before the identification is decided.

Art. 8.

(1) Operators of essential services shall take the necessary and proportionate technical and organisational measures to manage the risks to the security of the networks and information systems they use in the course of their business. These measures shall ensure a level of security for networks and information systems appropriate to the existing risk, taking into account the state of knowledge. In order to identify risks, operators of essential services shall use an appropriate risk analysis framework which may be specified by the relevant competent authority by way of regulation.

(2) Operators of essential services shall take appropriate measures to prevent or limit the impact of incidents that compromise the security of networks and information systems used for the provision of such essential services, with a view to ensuring the continuity of such services.

(3) Measures taken on the basis of paragraphs 1 and 2 shall be notified to the competent authority concerned. The modalities of such notification, the format and the time limit, shall be determined by the competent authority concerned by means of a regulation.

(4) Operators of essential services shall notify the relevant competent authority, without undue delay, of incidents that have a significant impact on the continuity of the essential services they provide. These notifications are forwarded to the Government CERT and the CIRCL according to their respective competencies. The notifications shall contain information enabling the competent authority concerned to determine whether the incident has a cross-border impact. Such notification shall not increase the liability of the party making it.

(5) The extent of the impact of an incident is determined by taking into account, in particular, the following parameters

1° the number of users affected by the essential service disruption;

2° duration of the incident;

3° the geographical scope in terms of the area affected by the incident.

The relevant competent authority may specify, by means of a regulation, the parameters, modalities and deadlines for the notification of incidents that have a significant impact on the continuity of the essential services they provide.

(6) On the basis of the information provided in the notification from the operator of essential services, the relevant competent authority shall inform the other affected Member States whether the incident is likely to have a significant impact on the continuity of essential services in those Member States. At the request of the competent authority concerned, this alert shall be made by the single national contact point, which will forward the notification to the national contact points of the other Member States affected. In doing so, the competent authority concerned must safeguard the security and commercial interests of the operator of essential services and the confidentiality of the information provided in its notification.

Where circumstances permit, the competent authority concerned shall provide the notifying operator of essential services with information relevant to the follow-up of its notification.

(7) Once a year, the competent authority concerned shall provide the single national contact point with a summary report on the notifications received, including the number of notifications and the nature of the incidents notified, and on the measures taken in accordance with paragraphs 4 and 6.

Each year, the single national contact point shall provide the cooperation group with a summary report on the notifications received, including the number of notifications and the nature of the incidents notified, and on the measures taken in accordance with paragraphs 4 and 6.

(8) After consultation with the notifying operator of essential services, the relevant competent authority may inform the public of specific incidents or require the operator of essential services to do so, where public awareness is necessary to prevent an incident or to manage an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

Art. 9.

(1) At the request of the competent authority concerned, operators of essential services shall provide:

1° the information necessary to assess the security of their networks and information systems, including documents relating to their security policies;

2° evidence of the effective implementation of security policies, such as the results of a security audit carried out by the relevant competent authority or a qualified auditor and, in the latter case, that they make the results, including evidence, available to the relevant competent authority. The competent authority concerned may appoint an external auditor to monitor the effective implementation of the

security policy by the operator of essential services;

3° any information necessary for the performance of its duties under this Act.

Operators of essential services shall provide such information within the time limits and at the level of detail required by the relevant competent authority.

When making such a request for information and evidence, the competent authority concerned shall state the purpose of the request and specify what information is required.

(2) After evaluation of the information or results of the security audits referred to in paragraph 1, the competent authority concerned may issue binding instructions to operators of essential services to remedy the identified deficiencies.

(3) In dealing with notified incidents involving breaches of personal data, the competent authority concerned shall cooperate closely with the National Data Protection Commission and shall forward to it information relating to such breaches.

Chapter 4 - Digital Service Providers

Art. 10.

(1) Digital service providers having their principal place of business in the Grand Duchy of Luxembourg shall fall within the scope of this Act. A digital service provider is deemed to have its principal place of business in the Grand Duchy of Luxembourg when its registered office is in the Grand Duchy of Luxembourg. A digital service provider who is not established in the European Union but who provides a digital service on the territory of the Grand Duchy of Luxembourg and who appoints a representative in the Grand Duchy of Luxembourg shall be subject to the jurisdiction of the Luxembourg authorities.

The representative may be contacted by the relevant competent authority instead of the digital service provider regarding the obligations of the digital service provider under this Act.

The appointment of a representative by the digital service provider is without prejudice to any legal action that may be brought against the digital service provider itself.

(2) Chapter 4 shall not apply to micro and small enterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

Art. 11.

(1) Digital service providers shall identify the risks to the security of the networks and information systems they use to provide a digital service in the European Union and take the necessary and proportionate technical and organisational measures to manage them. These measures shall ensure, taking into account the state of the art, a level of security of networks and information systems appropriate to the existing risk and shall take into account the following elements

1° system and facility security;

2° incident management;

3° business continuity management;

4° monitoring, audit and control;

5° compliance with international standards.

The management of risks that threaten the security of digital service providers' networks and information systems is done in accordance with Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down detailed rules for the implementation of Directive (EU) 2016/1148 of the European

Parliament and of the Council specifying the elements to be taken into account by digital service providers in managing risks that threaten the security of networks and information systems and the parameters for determining whether an incident has a significant impact.

(2) Digital service providers shall take measures to prevent security incidents on their networks and information systems and to minimise the impact of such incidents on digital services offered in the European Union, so as to ensure the continuity of such services.

(3) Digital service providers shall notify the relevant competent authority, without undue delay, of any incident that has a significant impact on the provision of a digital service they offer in the European Union. The terms of this notification, the format and the time limit, shall be determined by the competent authority concerned by means of a regulation. These notifications are forwarded to the Government CERT and the CIRCL according to their respective competencies. The notifications shall contain information enabling the competent authority concerned to assess the extent of the possible impact at cross-border level. Such notification shall not increase the liability of the party making it.

(4) The significance of the impact of an incident is determined by taking into account, in particular, the following parameters

1° the number of users affected by the incident, in particular those who use the service to provide their own services;

2° duration of the incident;

3° the geographical scope in terms of the area affected by the incident;

4° the severity of the disruption to the operation of the service;

5° the extent of the impact on economic and societal functions.

The obligation to notify an incident shall only apply where the digital service provider has access to the information necessary to assess the impact of the incident with regard to the parameters referred to in the first subparagraph.

The parameters for determining whether an incident has a significant impact are specified in Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down detailed rules for the implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council specifying the elements to be taken into account by digital service providers when managing risks to the security of networks and information systems and the parameters for determining whether an incident has a significant impact.

(5) Where an operator of essential services relies on a third-party digital service provider for the provision of a service essential to the maintenance of critical societal and economic functions, any significant impact on the continuity of essential services due to an incident affecting the digital service provider shall be notified by that operator.

(6) Where the incident referred to in paragraph 3 involves two or more Member States, the competent authority concerned may inform the other Member States affected. In doing so, the competent authority concerned must safeguard the security and business interests of the digital service provider and the confidentiality of the information provided.

(7) Once a year, the competent authority concerned shall provide the single national contact point with a summary report on the notifications received, including the number of notifications and the nature of the incidents notified, and on the measures taken in accordance with paragraphs 3 and 6.

Each year, the single national contact point shall provide the cooperation group with a summary report on the notifications received, including the number of notifications and the nature of the incidents notified, and on the measures taken in accordance with paragraphs 3 and 6.

(8) After consultation with the digital service provider concerned, the competent authority concerned, and

the authorities or CSIRTs of the other Member States concerned, may inform the public of particular incidents or require the digital service provider to do so, where public awareness is necessary to prevent an incident or to manage an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

Art. 12.

(1) The competent authority concerned may require digital service providers:

1° to provide it with the information necessary to assess the security of their networks and information systems, including documents relating to their security policies;

2° to remedy any breach of the obligations set out in Article 11;

3° to provide it with any information necessary for the performance of its duties under this Act.

(2) If a digital service provider has its principal place of business or a representative in the Grand Duchy of Luxembourg but its networks and information systems are located in one or more other Member States, the relevant Luxembourg competent authorities and the competent authorities of those other Member States shall cooperate closely and shall afford each other such assistance as may be necessary for the application of this law.

The obligation of professional secrecy provided for in Article 16 of the amended law of 23 December 1998 creating a Financial Sector Supervisory Commission and in Article 15 of the amended law of 30 May 2005 on: 1) organisation of the Institut Luxembourgeois de Régulation; 2) amendment of the amended law of 22 June 1963 fixing the salary system for State officials does not preclude such cooperation.

Chapter 5 - Voluntary Notification

Art. 13.

(1) Entities which have not been identified as operators of essential services and which are not digital service providers may notify, on a voluntary basis, incidents which have a significant impact on the continuity of the services they provide.

(2) When dealing with notifications, the competent authority concerned shall act in accordance with the procedure set out in Article 8. The competent authority concerned may treat mandatory notifications as having priority over voluntary notifications. Voluntary notifications shall be processed only where their processing does not impose a disproportionate or unnecessary burden on the competent authority concerned.

A voluntary notification shall not have the effect of imposing on the notifying entity any obligations to which it would not have been subject under this Law had it not made the notification.

Chapter 6 - Penalties

Art. 14.

(1) Where the competent authority concerned finds a breach of the obligations laid down in Articles 8, 9, 11 and 12 or by measures taken in implementation of this Act, it may impose one or more of the following penalties on the operator of essential services or digital service provider concerned:

1° a warning;

2° a reprimand;

3° a fine, the amount of which shall be proportionate to the seriousness of the infringement, the situation of the person concerned, the extent of the damage and the benefits derived therefrom but shall not exceed

EUR 125 000.

The fine may be imposed only if the infringements in question are not subject to a criminal penalty.

(2) Where it is established that a fact is likely to constitute an infringement as referred to in paragraph 1, the competent authority concerned shall initiate an adversarial procedure in which the operator of essential services or digital service provider concerned shall be given the opportunity to consult the file and to submit its written or oral observations. The operator of essential services or digital service provider concerned may be assisted or represented by a person of his choice. Following the adversarial procedure, the competent authority concerned may impose on the operator of essential services or digital service provider concerned one or more of the penalties referred to in paragraph 1.

(3) Decisions taken by the relevant competent authority following the adversarial procedure shall be reasoned and notified to the operator of essential services or digital service provider concerned.

(4) Against the decisions referred to in paragraph 3, an appeal for reversal shall be lodged with the Administrative Court.

(5) The collection of fines imposed by the ILR is entrusted to the Administration of Registration, Domains and VAT.

Chapter 7 - **Amending Provisions**

Art. 15.

In Article 2(y) of the amended Act of 20 April 2009 on the establishment of the State Information Technology Centre, the full stop shall be replaced by a semicolon, and Article 2 of the same Act completed as follows:

“z) the exercise, within the scope of these powers, of the function of Cryptographic Accreditation Authority, responsible for ensuring that cryptographic products comply with the respective cryptographic security policies; evaluating and accrediting cryptographic products for the protection of classified information up to a certain classification level in their operational environment; maintaining and managing technical data relating to cryptographic products."

Art. 16.

The Act of 23 July 2016 establishing a High Commission for National Protection is amended as follows:

1° In Article 2(4), the full stop shall be replaced by a semicolon and a new point 5 shall be inserted after point 4, reading as follows

“5. "National Network and Information Systems Security Strategy" means a framework setting out strategic objectives and priorities for network and information systems security at the national level;

2° In Article 3(1)(b), point 4 is added, worded as follows:

“4. to coordinate and develop a national network and information systems security strategy;";

3° In Article 8(1), "Article 5" is replaced by "Article 4";

4° After Article 9, a new Chapter 4a is inserted as follows

"Chapter 4bis - **The national strategy for network and information systems security**

Art. *9bis.*

The Office of the High Commissioner for National Protection is developing a national strategy for network and information systems security, which includes the following points

a) the objectives and priorities of the national network and information systems security strategy;

b) a governance framework to achieve the objectives and priorities of the national network and information systems security strategy, including the roles and responsibilities of government agencies and other relevant actors;

c) the inventory of preparedness, response and recovery measures, including cooperation between the public and private sectors;

d) an overview of education, awareness and training programs related to the national network and information systems security strategy;

e) an overview of research and development plans related to the national network and information systems security strategy;

f) a risk assessment plan to identify the risks;

g) a list of the different stakeholders involved in the implementation of the national network and information systems security strategy.

Art. 17.

This law shall enter into force on the first day of the second month following its publication in the Official Journal of the Grand Duchy of Luxembourg.

Mandate and order that the present law be inserted in the Official Gazette of the Grand Duchy of Luxembourg to be executed and observed by all those concerned by the matter.

The Prime Minister,

Minister of State,

Minister for Communications and Media,

Xavier Bettel

The Minister of Finance,

Pierre Gramegna

The Palace of Luxembourg, 28 May 2019.

Henri

Parl. Doc. 7314; Ord. sess. 2017-2018 and 2018-2019; Dir. (EU) 2016/1148.

ANNEX

Types of entities for the purposes of Article 2(3)

Sector	Sub-sector	Type of entities
1. Energy	a) Electricity	– Electricity companies within the meaning of Article 1 (14) of the Act of 1 August 2007 on the organisation of the electricity market, as amended, which perform the function of "supply" within the meaning of Article 1(21) of the same Act
		– Distribution system operators within the meaning of Article 1(24) of the amended Act of 1 August 2007 on the organisation of the electricity market
		– Transmission system operators within the meaning of Article 1 (25) of the amended Act of 1 August 2007 on the organisation of the electricity market
	b) Oil	– Oil Pipeline Operators
		– Operators of oil production, refining, processing, storage and transportation facilities
	c) Gas	– Supply companies within the meaning of Article 1 (14) of the amended Act of 1 August 2007 on the organisation of the natural gas market
		– Distribution system operators within the meaning of Article 1 (22) of the amended Act of 1 August 2007 on the organisation of the natural gas market
		– Transmission system operators within the meaning of Article 1 (24) of the amended Act of 1 August 2007 on the organisation of the natural gas market
		– Storage facility operators within the meaning of Article 1 (25) of the amended Act of 1 August 2007 on the organisation of the natural gas market
		– LNG facility operators within the meaning of Article 1 (23) of the amended Act of 1 August 2007 on the organisation of the natural gas market
		– Natural gas undertakings within the meaning of Article 1(15) of the amended Act of 1 August 2007 on the organisation of the natural gas market
		– Natural gas undertakings within the meaning of Article 1(15) of the amended Act of 1 August 2007 on the organisation of the natural gas market

2. Transportation	a) Air transport	– Air carriers within the meaning of Article 3(4) of Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 establishing common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002
		– Entities managing airports within the meaning of Article 2(1) of the Act of 23 May 2012 transposing Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges and amending: 1. the amended Law of 31 January 1948 on the regulation of air navigation 2) the amended law of 19 May 1999 having as its object a) to regulate access to the ground handling market at Luxembourg airport; b) to create a regulatory framework in the field of civil aviation security; and c) to establish a Directorate for Civil Aviation, airports, including the core network airports listed in Annex II, Section 2 of Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU, and entities operating ancillary facilities located at airports
		– Air traffic control services within the meaning of Article 2(1) of 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)
	b) Rail transport	– Infrastructure managers within the meaning of Article 2(3) of the amended Act of 10 May 1995 on railway infrastructure management
		– Railway undertakings within the meaning of Article 2(7) of the amended Act of 11 June 1999 on access to and use of railway infrastructure, including operators of service facilities within the meaning of Article 2(2) of the amended Act of 10 May 1995 on railway infrastructure management
	c) Transport by water	– Inland, maritime and coastal passenger and cargo shipping companies as defined in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, excluding ships operated by such companies on an individual basis
		– Entities managing ports within the meaning of Article 3(1) of Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security, including port facilities within the meaning of Article 2(11) of Regulation (EC) No 725/2004, as well as entities operating

		workshops and equipment within ports – Vessel traffic service operators within the meaning of Article 2(o) of the amended Grand Ducal Regulation of 27 February 2011 establishing a Community vessel traffic monitoring and information system
	d) Road transport	– Road authorities within the meaning of Article 2(12) of Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council as regards the provision of real-time traffic information services throughout the Union, responsible for traffic management control
		– Operators of smart transport systems within the meaning of the circular letter of 22 February 2012 concerning 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 transport modes
3. Credit institutions		– Credit institutions within the meaning of Article 1 (12) of the amended Law of 5 April 1993 on the financial sector
4. Financial Market Infrastructures		– Operators of trading platforms within the meaning of Article 1 (43) of the law of 30 May 2018 on markets in financial instruments
		– Central counterparties as defined in Article 2(1) of 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
5. Health sector	Health care facilities (including hospitals and private clinics)	– Health care providers within the meaning of Article 2(f) of the amended Act of 24 July 2014 on the rights and obligations of the patient
6. Supply and distribution of drinking water		– Suppliers and distributors of water intended for human consumption within the meaning of Article 3(1)(a) of the amended Grand Ducal Regulation of 7 October 2002 on the quality of water intended for human consumption
7. Digital infrastructure		– IXP
		– DNS Service Providers
		– Top Level Domain Registries