Law of 28 May 2019 transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the European Union

Law of 28 May 2019 transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the European Union and amending

1° the Law of 20 April 2009 establishing the Government IT Centre, as amended, and

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

(Mém. A 2019, No 372)

We Henri, Grand Duke of Luxembourg, Duke of Nassau,

Having heard our State Council;

With the consent of the Chamber of Deputies;

Having regard to the decision of the Chamber of Deputies of 15 May 2019 and that of the State Council of 21 May 2018 that a second vote is not required;

Ordered and order:

Chapter 1 - Definitions and Scope

Article 1.

(1) The security and notification requirements provided for in this Law shall not apply to undertakings which are subject to the requirements of Articles 45 and 46 of the amended Law of 27 February 2011 on electronic communication networks and services or to trust service providers which are subject to the requirements of 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 law or a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in this Law, the provisions of that sector-specific law or European Union legal act shall apply.

Article 2.

For the purposes of this Law, the following definitions shall apply:

1° "network and information system" means

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

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;

or

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (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 resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data and related services offered by, or accessible via, those network and information systems;

3° "operator of essential services" (or "OES") means a public or private entity of a type referred to in the Annex, which meets the criteria laid down in Article 7(2);

4° "digital service" means a service within the meaning of Article 1(1)(b) of the Law of 8 November 2016 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services of the "online marketplace", "online search engine" or "cloud computing service" type;

5° "digital service provider" means any legal person that provides a digital service;

6° "incident" means any event having an actual adverse effect on the security of network and information systems;

7° "incident handling" means all procedures supporting the detection, analysis and containment of an incident and the response thereto;

8° "risk" means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;

9° "representative" means any natural or legal person established in the European Union explicitly designated to act on behalf of a digital service provider not established in the European Union;

10° "standard" means a standard within the meaning of point (1) of Article 2 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" means a technical specification within the meaning of point (4) of Article 2 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 facility which enables 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 the internet traffic passing between any pair of

participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

13° "domain name system", hereinafter "DNS" means a hierarchical distributed naming system in a network which refers queries for domain names;

14° "DNS service provider" means an entity which provides DNS services on the internet;

15° "top-level domain name registry" means an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD);

16° "online marketplace" means a digital service that allows consumers or traders, as respectively defined in point (1) and in point (2) of Article L. 010-1 of the Consumer Code, to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;

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

18° "cloud computing service" means a digital service that enables access to a scalable and elastic pool of shareable computing resources;

19° "Governmental CERT" means the Governmental Computer Emergency Response Team, as defined in the Grand-ducal decree of 9 May 2018 defining the organisation and the duties of the Governmental Computer Emergency Response Team, also referred to as "CERT Gouvernemental";

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

21° "CSIRT" means the Computer Security Incident Response Team;

22° "Cooperation Group" means a group established in order to support and facilitate strategic cooperation and the exchange of information among Member States,to strengthen trust and confidence, with a view to achieving a high common level of security of networks and information systems in the European Union;

23° "CSIRTs network" means a group established to build confidence and trust between the Member States and to promote swift and effective operational cooperation;

24° "national single point of contact" means an authority that exercises a liaison function to ensure cross-border cooperation between Member State authorities, as well aswith the relevant authorities in other Member States, the Cooperation Group and the CSIRTs network.

Chapter 2 - Competent authorities concerned and national single point of contact

Article 3.

The Commission de Surveillance du Secteur Financier, hereinafter "the CSSF", shall be the competent authority on the security of network and information systems covering the credit institutions and financial market infrastructures sectors as defined under points (3) and (4) of the Annex, as well as the digital services provided by an entity subject to the CSSF's supervision.

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

The professional secrecy obligation provided for in Article 16 of the amended Law of 23 December 1998 establishing a financial sector supervisory commission ("Commission de surveillance du secteur financier") and Article 15 of the amended Law of 30 May 2005: 1) organising the l'Institut Luxembourgeois de Régulation; 2) amending the amended Law of 22 June 1963 laying down the salaries of civil servants shall not prevent competent authorities from exchanging information.

Article 4.

The ILR shall constitute the national single point of contact on the security of network and information systems.

Article 5.

The ILR shall receive a financial contribution from the State budget to cover all the operating costs resulting from the exercise of the missions provided for in this Law.

Article 6.

To the extent necessary for the purposes of conducting their mission pursuant to this Law, the competent authorities and the national single point of contact shall consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.

The professional secrecy obligation provided for in Article 16 of the amended Law of 23 December 1998 establishing a financial sector supervisory commission ("Commission de surveillance du secteur financier") and Article 15 of the amended Law of 30 May 2005; 1) organising the l'Institut Luxembourgeois de Régulation; 2) amending the amended Law of 22 June 1963 laying down the salaries of civil servants shall be without prejudice to this cooperation.

Chapter 3 - Operators of essential services

Article 7.

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

(2) Operators of essential services shall be identified by the relevant competent authority based on the following identification criteria:

1° an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

2° the provision of that service depends on network and information systems; and

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

The relevant competent authority shall notify the operator of essential services of its decision regarding the identification.

(3) When determining the significance of a disruptive effect as referred to in point (3) of paragraph 2, at least the following cross-sectoral and sector-specific factors shall be taken into account:

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

2° the dependency of other sectors referred to in the Annex on the service provided by that entity;

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

4° the market share of that entity;

5° the geographic spread with regard to the area that could be affected by an incident;

6° the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

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

(5) Where an entity provides a service as referred to in point (1) of paragraph 2 in another Member State, the relevant competent authority shall engage in consultation with the competent authority of the other Member State. The consultation shall take place before a decision regarding the identification is taken.

Article 8.

(1) Operators of essential services shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed. To identify the risks, the operators of essential services shall use an appropriate risk assessment framework which can be specified by the relevant competent authority by means of a regulation.

(2) Operators of essential services shall take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

(3) The measures taken based on paragraphs 1 and 2 shall be notified to the competent authority concerned. The modalities, format and deadline of such notification shall be determined by the relevant competent authority by means of a regulation.

(4) Operators of essential services shall notify, without undue delay, the relevant competent authority of incidents having a significant impact on the continuity of the essential services they provide. These notifications shall be transmitted to the Governmental CERT and the CIRCL according to their respective areas of responsibility. Notifications shall include information enabling the relevant competent authority to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

(5) In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:

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

2° the duration of the incident;

3° the geographical spread with regard to the area affected by the incident.

The relevant competent authority may specify, by means of a regulation, the parameters, modalities and deadlines relating to the notification of incidents having a significant impact on the continuity of the essential services provided by operators of essential services (or "OES").

(6) On the basis of the information provided in the notification by the operator of essential services, the relevant competent authority shall inform the other affected Member States if the incident is likely to have a significant impact on the continuity of essential services in these Member States. Upon request of the relevant competent authority, the national single point of contact shall inform other affected Member States by transmitting the notification to the national points of contact of these affected Member States. In doing so, the relevant competent

authority shall preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.

Where the circumstances allow, the relevant competent authority shall provide the notifying operator of essential services with useful information for the follow-up of its notification.

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

Every year, the national single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications, the nature of the notified incidents, and the measures taken in accordance with paragraphs 4 and 6.

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

Article 9.

(1) Upon request of the relevant competent authority, operators of essential services shall provide:

1° the information necessary to assess the security of their network and information systems, including documented 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, make the results thereof, including the underlying evidence, available to the relevant competent authority. The relevant competent authority may appoint an external auditor to verify the effective implementation of the security policy. The costs shall be borne by the operator of essential services;

3° any information necessary to fulfil its missions pursuant to this Law.

The operators of essential services shall provide this information according to the deadline set and level of detail required by the relevant competent authority.

When requesting such information or evidence, the relevant competent authority shall indicate the purpose of the request and specify the information required.

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

(3) The relevant competent authority shall work in close cooperation with the National Commission for Data Protection when addressing notified incidents resulting in personal data breaches and shall provide it with any information relating to these breaches.

Chapter 4 - Digital service providers

Article 10.

(1) Digital service providers having their main establishment in the Grand Duchy of Luxembourg shall fall within the scope of this Law. A digital service provider shall be deemed to have its main establishment in the Grand Duchy of Luxembourg when it has its head office in the Grand

Duchy of Luxembourg. A digital service provider that is not established in the European Union but offers digital services on the territory of the Grand Duchy of Luxembourg and designates a representative in the Grand Duchy of Luxembourg, shall fall within the competence of the Luxembourg authorities.

The representative may be addressed by the relevant competent authority instead of the digital service provider with regard to the obligations of that digital service provider pursuant to this Law.

The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated 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.

Article 11.

(1) Digital service providers shall identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering digital services within the European Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

1° the security of systems and facilities;

2° incident handling;

3° business continuity management;

4° monitoring, auditing and testing;

5° compliance with international standards.

The risks posed to the security of network and information systems shall be managed in accordance with Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

(2) Digital service providers shall take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the digital services that are offered within the European Union, with a view to ensuring the continuity of those services.

(3) Digital service providers shall notify the relevant competent authority, without undue delay, of any incident having a substantial impact on the provision of a digital service that they offer within the European Union. The modalities, format and deadline of such notification shall be determined by the relevant competent authority by means of a regulation. These notifications shall be transmitted to the Governmental CERT and the CIRCL according to their respective areas of responsibility. Notifications shall include information to enable the relevant competent authority to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.

(4) In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:

1° the number of users affected by the incident, in particular users relying on the service for the provision of their own services;

2° the duration of the incident;

3° the geographical spread with regard to the area affected by the incident;

4° the extent of the disruption of the functioning of the service;

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

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

The parameters for determining whether an incident has a substantial impact are specified in Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

(5) Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the 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 concerns two or more Member States, the relevant competent authority shall inform the other affected Member States. In doing so, the relevant competent authority shall preserve the security and commercial interests of the digital service provider, as well as the confidentiality of the information provided.

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

Every year, the national single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications, the nature of the notified incidents, and the measures taken in accordance with paragraphs 3 and 6.

(8) After consulting the digital service provider concerned, the relevant competent authority concerned, the authorities or the CSIRTs of other Member States concerned may inform the public about specific incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

Article 12.

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

1° provide the information necessary to assess the security of their network and information systems, including documented security policies;

2° remedy any failure to meet the requirements laid down in Article 11;

3° provide it with any information necessary to fulfil its missions pursuant to this Law.

(2) If a digital service provider has its main establishment or a representative in the Grand Duchy of Luxembourg, but its network 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 closely cooperate and assist each other to the extent necessary for the application of this Law.

The professional secrecy obligation provided for in Article 16 of the amended Law of 23 December 1998 establishing a financial sector supervisory commission ("Commission de surveillance du secteur financier") and Article 15 of the amended Law of 30 May 2005: 1) organising the l'Institut Luxembourgeois de Régulation; 2) amending the amended Law of 22 June 1963 laying down the salaries of civil servants shall be without prejudice to this cooperation.

Chapter 5 - Voluntary notification

Article 13.

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

(2) When processing notifications, the relevant competent authority shall act in accordance with the procedure set out in Article 8. The relevant competent authority may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on the relevant competent authority.

A voluntary notification shall not result in imposing upon the notifying entity obligations to which it would not have been subject pursuant to this Law had it not proceeded with that notification.

Chapter 6 – Sanctions

Article 14.

(1) Where the relevant competent authority records a breach of the obligations set out in Articles 8, 9, 11 and 12 or by measures taken in the implementation of this Law, it may impose one or more of the following sanctions on the operator of essential services or digital service provider concerned:

1° a warning;

2° a reprimand;

3° an administrative fine, the amount of which shall be proportionate to the severity of the breach, the situation of the person involved, the extent of the damage and benefits received without exceeding EUR 125,000.

The fine can only be imposed provided that the failures referred to above are not subject to criminal sanction.

(2) Where any fact is likely to be considered as a breach as referred to in paragraph 1, the relevant competent authority shall initiate an adversarial procedure, whereby the operator of essential services or the digital service provider concerned may access the file and submit observations in writing or orally. The operator of essential services or the digital service provider concerned may be assisted or represented by a person of its choice. On the outcome of the adversarial procedure, the relevant competent authority may impose on the operator of essential services

or the digital service provider concerned one or more of the sanctions referred to in paragraph 1.

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

(4) An action for reversal may be initiated against the decisions referred to in paragraph 3 before the *Tribunal administratif* (Administrative Tribunal).

(5) Collection of administrative fines imposed by the ILR shall be entrusted to the Registration Duties, Estates and VAT Authority.

Chapter 7 – Amending provisions[1]

Article 15.

(…)[2]

Article 16.

(…)[3]

Article 17.

This Law shall enter into force on the first day of the second month following its publication in the Journal officiel du Grand-Duché de Luxembourg.

We instruct and order that this Law be inserted in the Journal officiel du Grand-Duché de Luxembourg in order to be implemented and complied with by all the persons concerned.

Parl. doc. 7314; ord. sess. 2017-2018 and 2018-2019, Dir. (UE) 2016/1148.

[1] The amending provisions are not included in this version.

[2] The amending provisions are not included in this version.

[3] The amending provisions are not included in this version.

ANNEX

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

Sector	Subsector	Type of entities
1. Energy	(a) Electricity	- Electricity undertakings as defined in Article 1(14) of the amended Law of 1 August 2007 on the organisation of the electricity market, which carry out the function of "supply" as defined in Article 1(21) of the same law
		- Distribution system operators as defined in Article 1(24) of the amended Law of 1 August 2007 on the organisation of the electricity market
		- Transmission system operators as defined in Article 1(25) of the amended Law of 1 August 2007 on the organisation of the electricity market
	(b) Oil	- Operators of oil transmission pipelines
		- Operators of oil production, refining and treatment facilities, storage and transmission
	(c) Gas	- Supply undertakings as defined in Article 1(14) of the amended Law of 1 August 2007 on the organisation of the natural gas market
		- Distribution system operators as defined in Article 1(22) of the amended Law of 1 August 2007 on the organisation of the natural gas market
		- Transmission system operators as defined in Article 1(24) of the amended Law of 1 August 2007 on the organisation of the natural gas market
		- Storage system operators as defined in Article 1(25) of the amended Law of 1 August 2007 on the organisation of the natural gas market
		- LNG system operators as defined in Article 1(23) of the amended Law of 1 August 2007 on the organisation of the natural gas market
		- Natural gas undertakings as defined in Article 1(15) of the amended Law of 1 August 2007 on the organisation of the natural gas market
		- Operators of natural gas refining and treatment facilities

2. Transport	(a) Air transport	- Air carriers as defined in point (4) of Article 3 of 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
		- Airport managing bodies as defined in point (1) of Article 2 of the Law 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 aiming at a) regulating access to the ground-handling assistance market at Luxembourg Airport; b) creating 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 installations contained within airports
		- Traffic management control operators providing air traffic control (ATC) services as defined in point (1) of Article 2 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 as defined in point (3) of Article 2 of the amended Law of 10 May 1995 on the railway infrastructure management
		- Railway undertakings as defined in point (7) of Article 2 of the amended Law of 11 June 1999 on the railway infrastructure and its use, including operators of service facilities as defined in point (2) of Article 2 of the amended Law of 10 May 1995 on the rail infrastructure management
	(c) Water transport	- Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport 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, not including the individual vessels operated by those companies
		- Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security, including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports

		- Operators of vessel traffic services as defined in point (o) of Article 2 of the amended Grand-ducal Regulation of 27 February 2011 establishing a Community vessel traffic monitoring and information system
	(d) Road transport	- Road authorities as defined in point (12) of Article 2 of 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, responsible for traffic management control
		- Operators of Intelligent Transport Systems as defined in the circular letter of 22 February 2012 on 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
3. Credit institutions		- Credit institutions as defined in point (12) of Article 1 of the amended Law of 5 April 1993 on the financial sector
4. Financial market infrastructures		- Operators of trading venues as defined in point (43) of Article 1 of the Law of 30 May 2018 on markets in financial instruments
		- Central counterparties (CCPs) as defined in point (1) of Article 2 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 settings (including hospitals and private clinics)	- Healthcare providers as defined in point (f) of Article 2 of the amended Law of 24 July 2014 on the rights and obligations of the patient
6. Drinking water supply and distribution		- Suppliers and distributors of water intended for human consumption as defined in letter (a) of point (1) of Article 3 of the amended Grand-ducal Regulation of 7 October 2002 on the quality of water intended for human consumption
7. Digital Infrastructure		- IXPs
		- DNS service providers
		- TLD name registries