EnCaViBS

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

Member State:

Belgium

7 April 2019. Law Establishing a Framework for the Security of Network and Information Systems of General Interest for Public Security

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: Belgium

7 April 2019. Law Establishing a Framework for the Security of Network and Information Systems of General Interest for Public Security

C-2019/11507
Moniteur Belge 03.05.2019, 42857

PHILIPPE, King of the Belgians, To all, present and future, Greetings.

The House of Representatives has passed, and We do hereby sanction the following:

TITLE I. - Definitions and general provisions

CHAPTER I. - Purpose and scope

Section 1. - Purpose

Article 1. This Act regulates a matter referred to in Article 74 of the Constitution.

Art. 2.

The purpose of this Act is, inter alia, to transpose the European 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 security of networks and information systems in the Union, hereinafter referred to as the "NIS Directive".

Section 2. - Scope of application

Art. 3.
§ 1. This Act applies to operators of essential services, as defined in Article 6, 11°, having at least one establishment on Belgian territory and actually carrying out an activity related to the provision of at least one essential service on Belgian territory. The provisions of Title 1, Articles 13, 14 and 30 and Chapter 3 of Title 4 shall apply to potential operator of essential services.

§ 2. This Act applies to digital service providers, as defined in Article 6, 21°, whose principal place of business is in Belgium. A digital service provider is deemed to have its principal place of business in Belgium if its registered office is located there. This Act shall also apply to digital service providers which do not have an establishment in the European Union when they provide services in Belgium as referred to in Annex II and establish their representative in Belgium for the purposes of the NIS Directive.

Art. 4.

§ 1. The security and notification requirements provided for in this Act shall not apply, for their activities in providing public electronic communications networks or publicly available electronic communications services, to undertakings subject to the requirements set out in Articles 114 and 114/1 of the Act of 13 June 20052 on electronic communications, and, for their trust service activities, to trust service providers subject to the requirements set out in Article 19 of European 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 sectoral legal act of the European Union 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, and provided that the requirements in question have an effect at least equivalent to that of the obligations laid down in this Act, the provisions on the security of networks and information systems and incident reporting of that act may derogate from the provisions of this Act. The King is responsible for specifying any equivalent sectoral acts referred to in the first paragraph.

§ 3. This Act shall not apply to operators in the finance sector within the meaning of Annex I to this Act, with the exception of the provisions of Title I, Chapter 1 of Title II and Article 26. By way of derogation from paragraph 1, Article 52 is applicable to operators in the finance sector within the meaning of Annex I to this Act, with the exception of trading platform operators within the meaning of Article 3, 6°, of the Act of 21 November 2017 on the infrastructures of the markets in financial instruments and transposing Directive 2014/65/EU. Sectoral authorities and operators in the finance sector within the meaning of Annex I to this Act shall be subject to Articles 65 to 73. By way of derogation from the above, Articles 65 to 73 are not applicable to the sectoral authority concerned when the latter acts in the cases referred to in Article 46bis of the Law of 2 August 20026 on the supervision of the financial sector and financial services or in Article 12quater of the Law of 22 February 1998 laying down the organic status of the National Bank of Belgium.

§ 4. This Act shall not apply where and insofar as measures for the security of networks and information systems exist pursuant to the Act of 15 April 1994 on the protection of the population and the environment against the dangers arising from ionising radiation and on the Federal Nuclear Supervisory Agency. By way of derogation from paragraph 1, this Act shall apply to the components of a nuclear installation intended for the industrial production of electricity and used for the transmission of electricity.

Art. 5.

§ 1. Subject to the provisions of Title 6, this Act is without prejudice to the application of EU Regulation 2016/679, or to the legal and regulatory provisions that complement or specify said Regulation.

§ 2. This Act is without prejudice to the application of the Act of 1 July 2011 on the security and protection of critical infrastructure, Articles 259bis, 314bis, 380, 382quinquies, 383bis, 383bis/1, 433septies, 433novies/1, 458bis, 550bis and 550ter of the Criminal Code, or other provisions of Belgian law transposing Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse, sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA, and Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

§ 3. This Act shall be without prejudice to the rules applicable to the processing of information, documents or data, equipment, materials or substances in any form whatsoever which are classified pursuant to the Act of 11 December 19984 on classification and security clearances, certificates and advice.

§ 4. This Act is without prejudice to the rules applicable to nuclear documents within the meaning of the Act of 15 April 1994 on the protection of the public and the environment against the dangers arising from ionising radiation and on the Federal Nuclear Control Agency.

CHAPTER 2. - Definitions

Art. 6.

For the purposes of this Act, the following definitions apply

(1) "National CSIRT" means the National Computer Security Incident Response Centre, designated by the King;

(2) "sectoral authority" means the public authority designated by law or by the King by decree deliberated in the Council of Ministers;

(3) "Sector CSIRT" means the sectoral computer security incident response centre, designated by the King;

(4) "personal data supervisory authority" means a supervisory authority within the meaning of Article 4, 21°, of Regulation EU 2016/679 of 27 April 2016 on the protection of individuals 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);

(5) "conformity assessment body" means a body referred to in Article I.9.7 of the Code of Economic Law;

(6) "certification audit" means an audit carried out in the context of a certification referred to in Article 22(2);

(7) "national accreditation authority" means a body established by the King in accordance with Article VIII.30 of the Code of Economic Law;

(8) "network and information system":

a) an electronic communications network within the meaning of Article 2, 3° of the Act of 13 June 20052 on electronic communications;

b) any device or set of interconnected or related devices, whether permanent or temporary, one or more of which, in execution of a program, performs automated processing of digital data, including the digital, electronic or mechanical components of the device, enabling, in particular, automation of the operational process, remote control, or obtaining real-time operating data;

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

(9) "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;

(10) "National Network and Information Systems Security Strategy": a framework of strategic objectives and priorities for network and information systems security at national level;

(11) "operator of essential services" means a public or private entity active in Belgium in one of the sectors listed in Annex I to this Act, which meets the criteria referred to in Article 12(1) and which is designated as such by the sectoral authority;

(12) "incident" means any event having an actual negative impact on the security of networks and information systems;

(13) "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;

(14) "risk" means any reasonably identifiable circumstance or event with a potential negative impact on the security of networks and information systems;

(15) "cross-sectoral criterion" means a factor common to all sectors listed in Annex I to this Act and determining the significance of a disruptive effect on the provision of an essential service within the meaning of Article 12(1)(c);

(16) "sectoral criterion" means a factor specific to a sector or subsector referred to in Annex I to this Act which determines the significance of a disruptive effect on the provision of an essential service within the meaning of Article 12(1)(c);

(17) "information systems and network security policy (ISNSP)" means a document referred to in Article 21(1) setting out the network and information systems security measures adopted by an operator of essential services;

(18) "information systems and network security contact point" means the contact point designated by the operator of essential services or digital service provider and which acts as a contact point vis-à-vis the authorities referred to in Article 7 for all matters relating to the security of the networks and information systems on which the essential services provided depend.

(19) "digital service" means a service within the meaning of Article 1(1)(b) of European Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and rules on information society services and the type of which is listed in Annex II;

(20) "digital service provider" means a legal entity who provides a digital service referred to in Schedule II to this Act;

(21) "representative of a digital service provider" means a natural or legal person established in Belgium who is expressly designated to act on behalf of a digital service provider not established in the Union, who may be contacted by the national authority referred to in Article 7(1), by the sectoral authority or by the competent inspection service in the place of the digital service provider concerning its obligations under this Act;

(22) "Internet Exchange Point (IXP)" means a network structure that allows the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of Internet traffic; an Internet Exchange Point interconnects only autonomous systems; an Internet Exchange Point does not require Internet traffic passing between two participating autonomous systems to transit through a third autonomous system, nor does it otherwise modify or alter such traffic;

(23) "domain name system" or "DNS" means a hierarchical, distributed system of assigning names in a network that resolves domain name issues;

(24) "DNS service provider" means an entity that provides DNS services on the Internet;

(25) "top-level domain registry" means an entity that registers and manages Internet domain names in a given top-level domain;

(26) "online marketplace" means a digital service that enables consumers within the meaning of Article I.1, first paragraph, 2°, of the Code of Economic Law and/or undertakings within the meaning of Article I.8, 39°, of the same Code to conclude online sales or service contracts with undertakings, either on the website of the online marketplace or on the website of an undertaking that uses the computer services provided by the online marketplace;

(27) "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 it is possible to find information related to the content requested;

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

(29) "Act of 1 July 2011" means the Act of 1 July 2011 on the security and protection of critical infrastructure;

(30) "Act of 11 December 19984" means the Act of 11 December 19984 on classification and security clearances, certificates and notices;

(31) "Act of 15 April 1994" means the Act of 15 April 1994 on the protection of the population and the environment against the dangers arising from ionising radiation and on the Federal Nuclear Control Agency;

(32) "EU Regulation 2016/679" means the European Regulation 2016/679 of 27 April 2016 on the protection of individuals 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).

CHAPTER 3. - Competent authorities and cooperation at national level

Section 1. - Competent authorities

Art. 7.

§ 1. The King shall designate the authority responsible, as the national authority, for monitoring and coordinating the implementation of this law. The authority referred to in paragraph 1 is also the single national contact point for network and information systems security for all operator of essential services and digital service providers for Belgium in its relations with the European Commission, the Member States of the European Union, the Cooperation Group referred to in Article 11 of the NIS Directive and the CSIRT network. To this end, the contact point represents Belgium in the Cooperation Group.

§ 2. The King shall designate the authority to act as the national CSIRT. The national CSIRT represents Belgium in the CSIRT network referred to in Article 12 of the NIS Directive. It cooperates effectively, efficiently and securely with the CSIRT network.

§ 3. The King shall designate, by decree deliberated in the Council of Ministers, the sectoral authorities responsible, for their respective sectors, for ensuring the implementation of the provisions of this law. The King may create sectoral authorities, composed of representatives of the Federal State, the Communities and the Regions, in accordance with the procedures set out in Article 92ter of the special law of 8 August 1980 on institutional reforms. By way of derogation from paragraph 1, the law itself designates the sectoral authorities created and regulated by the law.

§ 4. The King shall designate the authority responsible, in cooperation with the national authority referred to in paragraph 1, for coordinating the identification of operators of essential services.

§ 5. An inspection service per sector, or, where appropriate, per sub-sector, shall be set up, responsible for monitoring compliance with the provisions of this Act and its implementing acts by operators of essential services or by digital service providers.

The King shall designate, for a given sector or, where appropriate, by sub-sector, the inspection service competent to carry out the inspection.

By way of derogation from paragraph 2, the law shall designate the inspection services established and

governed by it.

Section 2. - Cooperation at the national level

Art. 8.

§ 1. The authorities referred to in Article 7 shall cooperate closely in order to comply with the obligations set out in this Law.

§ 2. According to the needs necessary for the execution of the law and in accordance with the applicable legal provisions, the authorities referred to in paragraph 1 shall also cooperate, at national level, with the administrative services of the State, the administrative authorities, the judicial authorities, the intelligence and security services referred to in the Organic Law of 30 November 19983 on the intelligence and security services, the police services referred to in the Law of 7 December 1998 organising an integrated police service, structured at two levels, and with the authorities responsible for the control of personal data.

§ 3. The operator of essential services, the digital service provider and the authorities referred to in Article 7 shall at all times collaborate by means of an appropriate exchange of information concerning the security of information systems and networks.

CHAPTER 4 - Information exchange

Art. 9.

§ 1. This article shall be without prejudice to the application of the Act of 11 December 1984, the Act of 15 April 1994, the Act of 11 April 1994 on the publicity of the administration or other legal provisions guaranteeing the confidentiality of information relating to the essential interests of national public security.

The authorities referred to in Article 7, the operator of essential services, the digital service provider, or their subcontractors shall limit access to information relating to the implementation of this Act to persons who need to know and have access to it for the performance of their functions or duties in connection with this Act.

§ 2. The staff members of the operator of essential services, the digital service provider, or their subcontractors shall be bound by professional secrecy with regard to information relating to the implementation of this Act.

Persons who are entrusted by their status or profession with secrets are authorized to make such secrets known for the purposes of this Act.

§ 3. The information provided to the authorities referred to in Article 7 by operator of essential services and digital service providers may be exchanged with authorities in the European Union, with Belgian or foreign authorities, when this exchange is necessary for the application of legal provisions.

The information exchanged is limited to what is relevant and is proportionate to the purpose of that exchange, including compliance with EU Regulation 2016/679. This exchange of information shall preserve the confidentiality of the information concerned and protect the security and commercial interests of operator of essential services and digital service providers.

CHAPTER 5. - National network and information systems security strategy

Art. 10.

§ 1. The King shall designate, by order deliberated in the Council of Ministers, the authority responsible for

keeping the existing national strategy for network and information system security up to date.

§ 2. The strategy referred to in paragraph 1 shall be updated, after obtaining the opinion of the authorities referred to in Article 7 and, where appropriate, of the personal data supervisory authorities. It shall cover at least the sectors listed in Annex I and the services listed in Annex II. This strategy defines the appropriate policy and regulatory objectives for achieving and maintaining a high level of network and information system security.

§ 3. The national network and information systems security strategy includes the following:

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 tasks 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 actors involved in the implementation of the national network and information systems security strategy.

TITLE 2. - Networks and information systems of operator of essential services

CHAPTER 1. - Identification of operator of essential services

Art. 11.

§ 1. The sector authority shall identify the operators of essential services in its sector, taking into account at least the types of operators listed in Annex I to this Law. Within the limits of their respective competences, the authorities referred to in Article 7 §§ 1 and 4 shall consult with the sectoral authority in order to carry out this identification. The sectoral authority shall, where appropriate, consult the regions or communities concerned and the representatives of the entities referred to in Annex I.

§ 2. After consultation with the potential operator of essential services, the sectoral authority shall specify the service or services designated as essential among the various services it provides.

§ 3. The sectoral authority will ensure the permanent monitoring of the process of identifying and designating operator of essential services and their essential services, in accordance with the procedures described in this chapter, with this process being carried out for the first time, at the latest, within six months of the entry into force of this Act. The sectoral authority shall assess and, where necessary, update the identification of operator of essential services and their essential services at least every two years. Updates shall be sent to the authorities referred to in Article 7 §§ 1 and 4.

Art. 12.

§ 1. To identify the operators referred to in Article 11, the sectoral authority shall apply the following criteria:
a) the entity provides a service that is essential to the maintenance of critical societal and/or economic activities;
b) the provision of this service is dependent on networks and information systems; and
c) an incident would be likely to have a significant disruptive effect on the provision of that service, taking

into account the criteria and impact levels or thresholds referred to in Article 13.

§ 2. In the absence of evidence to the contrary, the provision of an essential service is presumed to be dependent on networks and information systems.

Art. 13.

§ 1. In order to determine the significance of the disruptive effect referred to in Article 12(1)(c), the sectoral authority shall establish, for its sector, sectoral and/or cross-sectoral criteria, impact levels or thresholds. A significant disruptive effect is established as soon as the potential operator of essential services meets either a threshold or an impact level. Within the limits of their respective competences, the authorities referred to in Article 7(1) and (4) shall consult with the sectoral authority to determine the criteria, impact levels and thresholds, where appropriate, after consultation with the regions or communities concerned and representatives of the entities referred to in Annex I.

§ 2. The sectoral authority shall take into account at least the following cross-cutting criteria, based on available information:

a) the number of users dependent on the service provided by the entity concerned;

b) the dependence of other Annex I sectors on the service provided by that entity;

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

d) the market share of this entity;

e) the size of the geographical area likely to be affected by an incident;

f) 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.

§ 3. After obtaining the opinion of the authorities referred to in Article 7 and consulting the regions and communities concerned, the King may add to these intersectoral criteria.

Art. 14.

The potential operator of essential services shall, at the request of an authority referred to in Article 7, provide all relevant information concerning its possible identification as an operator of essential services, including information enabling the dependence or otherwise of the provision of the essential service on information networks and systems to be objectively determined. The relevant information transmitted by the potential operator shall be made known to the other authorities referred to in Article 7.

Art. 15.

§ 1. The sectoral authority shall communicate to the authorities referred to in Article 7(1) and (4) a reasoned proposal for a list of operators of essential services in its sector with the identification criterion(s) adopted. Where no operator of essential services has been proposed within a sector or sub-sector, the sectoral authority shall state its reasons in writing. The authorities referred to in Article 7(1) and (4) shall, within the limits of their respective competences, deliver an opinion on the reasoned proposal for a list, where appropriate after consulting the regions and communities.

§ 2. Where the sectoral authority finds that the entity it intends to designate as an operator of essential services provides one or more essential services in at least one other Member State of the European Union, it shall inform the authorities referred to in Article 7, §§ 1 and 4. The latter, in collaboration with the relevant sectoral authorities, shall organise discussions with the relevant foreign national authority or authorities and, where appropriate, with the regions or communities concerned.

§ 3. The sectoral authority shall notify the operator of its reasoned decision to designate it as an operator of essential services. This notification is done in a secure manner. It shall also send a copy of this decision to the authorities referred to in Article 7 §§ 1 and 4. The sectoral authority shall, where appropriate, inform the

regions and/or communities concerned.

Art. 16.

Within three months of its designation, the operator of essential services shall provide the sectoral authority with a description of the networks and information systems on which the provision of the essential service(s) concerned depends. The sectoral authority shall communicate this description to the authority referred to in Article 7(1).

Art. 17.

Without prejudice to the possible application of the Act of 11 December 1998 4, administrative documents related to the application of this chapter are considered to be administrative documents related to the safety of the population, public order and security, within the meaning of Article 6, § 1, of the Act of 11 April 1994 on the publicity of the administration, which may not be consulted, explained or communicated in the form of a copy to the public.

Art. 18.

§ 1. By way of derogation from Article 11, the sectoral authority shall designate operators of critical infrastructure, as designated under Article 8 of the Act of 1 July 2011 and Article 6 of the Royal Decree of 2 December 2011 on critical infrastructure in the air transport sub-sector, as operators of essential services when their sector is listed in Annex I to this Act and the provision of the essential services they provide is dependent on networks and information systems. This appointment shall be made in consultation with the authorities referred to in Article 7 §§ 1 and 4, within the limits of their respective competencies.

§ 2. In the absence of evidence to the contrary, the operation of a critical infrastructure is presumed to be dependent on networks and information systems.

§ 3. The operator shall provide the sectoral authority, at the request of the latter or of the authorities referred to in Article 7(1) and (4), with all relevant information concerning its possible identification as an operator of essential services, including information that makes it possible to objectively determine its dependence or otherwise on information networks and systems. The relevant information provided by the operator shall be communicated by the sectoral authority to the authorities referred to in Article 7 §§ 1 and 4.

§ 4. Article 15(3) shall apply to the reasoned decision to designate a critical infrastructure operator as an operator of essential services.

Art. 19. The King may, by decree deliberated in the Council of Ministers, add other sectors or types of operators to Annex I to this Law.

CHAPTER 2. - Safety measures

Art. 20.

The operator 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 on which its essential services depend. These measures shall ensure a level of physical and logical security for networks and information systems appropriate to the existing risks, taking into account the state of technical knowledge. The operator shall also take appropriate measures to prevent incidents that compromise the security of networks and information systems used for the provision of these essential services or to limit their impact, with a view to ensuring the continuity of these services.

Art. 21.

§ 1. The operator of essential services shall draw up a security policy for its information systems and networks

(hereinafter referred to as the "ISP"), which shall include at least the objectives and concrete security measures referred to in Article 20.

§ 2. The essential services operator shall draw up its ISP at the latest within twelve months of the notification of its designation. Within a period of twenty-four months at the latest from the date of notification of his designation, he shall implement the measures provided for in his I.S.P. For a given sector or, if necessary, by sub-sector, the competent sectoral authority may modulate this period according to the type of measures provided for in the IP.

§ 3. After obtaining the opinion of the authorities referred to in Article 7 and, where appropriate, after consulting the regions or communities concerned, the King may impose certain security measures applicable to operators of essential services in one or more sectors.

§ 4. The sectoral authority, in consultation with the authority referred to in Article 7, § 1, and, where appropriate, after consulting the regions or communities, may, by individual administrative decision, impose additional safety measures.

§ 5. The physical and logical security measures for networks and information systems contained in the operator's security plan (P.S.E.) referred to in Article 13 of the Act of 1 July 2011 and in Article 11 of the Royal Decree of 2 December 2011 concerning critical infrastructure in the air transport sub-sector shall be assimilated to the P.S.I. when all the information referred to in paragraph 2 is included therein.

Art. 22.

§ 1. The ISP referred to in Article 21, § 1 is, until proven otherwise, presumed to comply with the security requirements referred to in Article 20, when the security measures it contains meet the requirements of the ISO/IEC 27001 standard or a national, foreign or international standard recognised as equivalent by the King, by decree deliberated by the Council of Ministers. The decree referred to in the first paragraph shall be issued after obtaining the opinion of the national accreditation authority, the sectoral authority and the authority referred to in Article 7, § 1.

§ 2. Compliance with the requirements referred to in paragraph 1 shall be established by a certificate issued by a conformity assessment body accredited to ISO/IEC 17021 or ISO/IEC 17065 by the national accreditation authority or by an institution which is a co-signatory to the recognition arrangements of the European Cooperation for Accreditation. The certificate issued shall be within the scope of certification for which the conformity assessment body has been accredited and shall cover the entire contents of the ISP.

Art. 23.

§ 1. The operator of essential services shall designate its contact point for the security of information systems and networks and communicate its data to the competent sectoral authority within three months of notification of designation as an operator of essential services and without delay after each update of those data. The sectoral authority shall make these data available to the authorities referred to in Article 7(1) and (4).

§ 2. Where a security contact point already exists under national or international provisions applicable in a sector or subsector, the operator of essential services shall communicate its contact details to the sectoral authority within the time limits referred to in paragraph 1.

§ 3. The contact point for the security of information systems and networks referred to in paragraph 1 shall be available at all times.

CHAPTER 3. - Incident reporting

Art. 24.

§ 1. The operator of essential services shall notify, without delay, all incidents having a significant impact on

the availability, confidentiality, integrity or authenticity of the networks and information systems on which the essential service(s) it provides depend.

§ 2. After receiving the opinion of the national CSIRT, the authority referred to in Article 7, § 4, the sectoral authority and, where appropriate, the regions or communities concerned, the King may establish impact levels and/or thresholds, by sector or sub-sector, constituting at least a significant impact within the meaning of § 1.

§ 3. In the absence of the impact levels and/or thresholds referred to in paragraph 2, the operator shall notify all incidents having an impact on the availability, confidentiality, integrity or authenticity of the networks and information systems on which the essential service(s) it provides depend.

§ 4. The King can create different notification categories depending on the degree of impact of the incident.

Art. 25.

The notification referred to in Article 24 shall be made simultaneously to the national CSIRT, to the sectoral authority or its sectoral CSIRT and to the authority referred to in Article 7 § 4. The obligation to notify shall apply even if the operator of essential services has only part of the information relevant for assessing the significance of the impact of the incident.

Art. 26.

§ 1. This chapter applies to trading platform operators within the meaning of Article 3, 6°, of the Law of 21 November 2017 on infrastructures for markets in financial instruments and transposing Directive 2014/65/EU.

§ 2. Operators in the financial sector within the meaning of Annex I to the Act, with the exception of trading platform operators, shall notify the National Bank of Belgium (NBB), without delay, of all incidents having a significant impact on the availability, confidentiality, integrity or authenticity of the networks and information systems on which the essential service(s) they provide depend. The National Bank of Belgium shall determine the significant impact referred to in this paragraph. The NBB shall then forward the notification, without delay, to the national CSIRT and to the authority referred to in Article 7, § 4.

Art. 27.

An undertaking that provides a digital service to an operator of essential services and that is subject to this Act shall notify it, without delay, of all incidents that have a significant impact, within the meaning of Article 24, on the continuity of the latter's essential services. The essential services operator shall then notify this incident, following the procedures described in this chapter.

Art. 28.

§ 1. Where an operator of essential services is affected by an incident with a significant impact within the meaning of Article 24, the operator shall be obliged to manage the incident and take reactive measures to resolve it. Management of the incident remains the responsibility of the essential services operator.

§ 2. The operator of essential services shall investigate suspicious incidents or events notified to it by the national CSIRT, the sectoral authority or the authority referred to in Article 7(4).

Art. 29.

On the basis of the information provided in the notification from the operator of essential services, the national CSIRT shall inform the other affected EU Member States whether the incident has a significant impact on the continuity of essential services in those Member States. In doing so, the national CSIRT shall, in accordance with Union law or national legislation consistent with Union law, safeguard the security and commercial interests of the operator of essential services and the confidentiality of the information provided in its notification. The national CSIRT shall forward the notifications referred to in the first paragraph to the

single contact points of the other Member States affected.

Art. 30.

§ 1. Potential operator of essential services may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services they provide. A voluntary notification shall not have the effect of imposing on the notifying entity obligations to which it would not have been subject if it had not made the notification.

§ 2. When processing notifications, the national CSIRT, the sectoral authority or its sectoral CSIRT, and the authority referred to in Article 7, § 4, may give priority to mandatory notifications imposed by this law over notifications Voluntary notifications shall only be processed when their processing does not place a disproportionate or unnecessary burden on the national CSIRT, the sectoral authority or its sectoral CSIRT, and the authority referred to in Article 7, § 4.

Art. 31.

§ 1. The King is responsible for determining the modalities of notification and reporting of incidents, and for creating a secure reporting platform. This platform may also allow operators of essential services to notify supervisory authorities of personal data breaches, as imposed by Article 33(1) of Regulation EU 2016/679.

§ 2. After consultation with the notifying operator and the relevant sectoral authority, the national CSIRT may inform the public about specific incidents, where public awareness is necessary to prevent an incident or to manage an ongoing incident. This information is for general incident information only.

TITLE 3. - Networks and information systems of digital service providers

CHAPTER I. - Scope of application

Art. 32.

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

CHAPTER 2. - Security requirements

Art. 33.

§ 1. Digital service providers shall identify the risks to the security of the networks and information systems they use to provide the services referred to in Annex II within the 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

a) system and facility security;

b) incident management;

c) business continuity management;

d) monitoring, audit and control;

e) compliance with international standards.

§ 2. Digital service providers shall also take measures to prevent incidents affecting the security of their networks and information systems and to minimise the impact of such incidents on the services referred to in Annex II to this Act that are offered in the European Union, so as to ensure the continuity of such

services.

Art. 34.

Digital Service Providers shall inform a contact point for IT security and communicate the data to the competent sectoral authority for digital service providers, as well as after each update of these data. The sectoral authority shall communicate this information to the national authority referred to in Article 7(1).

CHAPTER 3. - Incident reporting

Art. 35.

§ 1. Digital service providers shall notify, without delay, any incident that has a significant impact on the provision of an Annex II service that they offer in the European Union. The notification shall be made simultaneously to the national CSIRT, the sectoral authority or its sectoral CSIRT and the authority referred to in Article 7(4) via the notification platform referred to in Article 31.

§ 2. Notification is done in accordance with the European Commission's implementing regulations, including that of 30 January 2018 2018/151 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. The notifications shall contain the information necessary to assess the extent of the possible impact at transboundary level. Such notification shall not increase the liability of the party making it.

§ 3. The obligation to notify an incident only applies when the digital service provider has access to the information necessary to assess, in full or in part, the impact of the incident.

Art. 36.

§ 1. Such notification shall be made in accordance with the procedures laid down by the King and via the platform referred to in Article 31.

§ 2. The platform referred to in Article 31 may also allow digital service providers to notify supervisory authorities of personal data breaches, as imposed by Article 33(1) of Regulation EU 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Art. 37.

§ 1. Where appropriate, and in particular if the incident referred to in Article 35(1) involves at least one other Member State of the European Union, the national CSIRT shall inform the other Member State(s) affected. In doing so, the national CSIRT must, in accordance with national and Union law, safeguard the security and commercial interests of the digital service provider and the confidentiality of the information provided.

§ 2. After consulting the digital service provider concerned, the sectoral authority and, where appropriate, the authorities or CSIRTs of the other EU Member States concerned, the national CSIRT may inform the public of particular incidents or require the digital service provider to do so. This information may be necessary, for example, where public awareness would prevent an incident or manage an ongoing incident, or where disclosure of the incident is in the public interest in other respects.

TITLE 4 - Checks and penalties

CHAPTER 1. - Checks on operators of essential services

Section 1. - Audits

Art. 38.

§ 1. The operator of essential services shall carry out an annual internal audit at its own expense of the networks and information systems on which the essential services it provides depend. This internal audit must enable the essential services operator to ensure that the measures and processes defined in its I.S.P. are well applied and are subject to regular controls. The operator of essential services shall forward the internal audit reports to the sectoral authority within 30 days.

§ 2. The operator of essential services shall have an external audit carried out, at least every three years and at its own expense, by a conformity assessment body accredited by the national accreditation authority, or by an institution which is a co-signatory to the recognition agreements of the European Cooperation for Accreditation. The operator of essential services shall forward the external audit reports to the sectoral authority within 30 days.

§ 3. At the latest within three months of drawing up its ISP, the essential services operator carries out its first internal audit. No later than 24 months after its first internal audit, the operator of essential services shall carry out its first external audit.

Art. 39.

§ 1. After obtaining the opinion of the sectoral authority and the authority referred to in Article 7, § 1, the King shall determine: 1° the general conditions of accreditation based on the requirements of ISO/IEC 17021 or ISO/IEC 17065;2° the additional sectoral requirements to which the conformity assessment body may be subject;3° the rules applicable to the internal audit;4° the rules applicable to the external audit.

§ 2. By decree deliberated in the Council of Ministers, the King may also determine, after obtaining the opinion of the sectoral authority and the authority referred to in Article 7, § 1, the conditions of any approval granted by the sectoral authority to a conformity assessment body.

§ 3. The list of accredited or approved conformity assessment bodies is available from the sectoral authority and is kept up to date.

Art. 40.

§ 1. Certification audits may be assimilated by the inspection service or the sectoral authority to the compulsory annual internal audit referred to in 39, § 1. The reports of these audits shall be transmitted by the operator of essential services to the sectoral authority within 30 days.

§ 2. Certification audits may be assimilated by the inspection service or the sectoral authority to the mandatory external audit referred to in Article 39(2). The reports of these audits shall be transmitted by the operator of essential services to the sectoral authority within 30 days.

Art. 41.

The authority referred to in Article 7(1) may request the sectoral authority or the inspection service, giving reasons, to transmit the certification or audit reports of an operator of essential services.

Section 2. - Inspection Service

Art. 42.

§ 1. The inspection services may at any time carry out checks on the compliance of the operator of essential services with the security measures and the incident reporting rules.

§ 2. The authority referred to in Article 7(1) or the sectoral authority may recommend, with reasons, that the inspection service carry out checks. After receiving the opinion of the sectoral authority and the authority referred to in Article 7, § 1, the King may lay down any practical sectoral arrangements for supervision.

§ 3. When making a request for information or evidence, the inspection service shall state the purpose of the request and the time limit within which the information or evidence must be provided. The inspection service may call on experts.

Art. 43.

When the networks and information systems of an operator of essential services are located outside Belgian territory, the inspection service, in consultation with the authority referred to in Article 7, § 1, may request the cooperation and assistance of the competent supervisory authorities of these other States. Such assistance and cooperation may include exchanges of information and requests for enforcement action.

Art. 44.

§ 1. The members of the inspection service shall be issued with a legitimation card, the model of which shall be determined by the King, by sector or, where applicable, by sub-sector.

§ 2. Members of the inspection service or experts called upon to take part in the inspection may not have any interest, direct or indirect, in the undertakings or institutions which they are responsible for inspecting, which could compromise their objectivity. They take an oath of office with the senior official in their department.

§ 3. Without prejudice to the powers of the judicial police officers referred to in Article 8 of the Code of Criminal Procedure, the sworn members of the inspection service shall have the following powers of control at all times in the exercise of their duties, both in the context of administrative procedures and in the context of the recording of offences:

1. To enter without prior warning, on presentation of their legitimation card, all premises used by the operator of essential services; they may only enter inhabited premises with prior authorisation issued by the investigating judge;

2. To examine on the spot and obtain a copy of the S.I.P., audit reports, any act, any document and any other source of information necessary for the performance of their duties;

3. To carry out any examination, check and hearing, and to request any information they consider necessary for the performance of their mission;

4. To take the identity of persons who are on the premises used by the essential services operator and whom they consider necessary to interview for the performance of their mission. To this end, they may require such persons to produce official identification documents;

5. To request the assistance of the federal or local police;

6. to request information from the members of staff referred to in Article 9 of the Act of 15 April 1994, for the purposes of implementing the provisions of this Act and the Act of 1 July 2011.

§ 4. In order to obtain permission to enter inhabited premises, the staff of the inspection service shall submit a reasoned request to the investigating judge. This application shall contain at least the following data:

1) identification of the inhabited spaces to which the staff of the inspection service or sectoral authority wish to have access;

2) the possible infringements which are the subject of the control;

3) all the documents and information from which it appears that the use of such means is necessary. The examining magistrate shall decide within a maximum of 48 hours of receiving the request. The decision of the investigating judge shall be reasoned. In the absence of a decision within the prescribed time limit, the visit to the premises shall be deemed to have been refused. The inspection service may appeal against the

refusal decision or the absence of a decision to the Indictment Division within 15 days of the notification of the decision or the expiry of the time limit. Visits without the occupant's permission to inhabited premises shall be carried out between five and twenty-one hours by at least two members of the inspection service acting jointly.

§ 5. At the beginning of any hearing, the person being questioned shall be informed: 1) that his statements may be used as evidence in court;

2) that it may request that all questions put to it and the answers it gives be recorded in the terms used;

3) that he has the right to remain silent and not to contribute to his own incrimination. Any person questioned may use the documents in his possession, without this leading to the postponement of the hearing. It may, at the time of the hearing or subsequently, require that these documents be attached to the hearing. The hearing shall state precisely the time at which it began, shall be interrupted and resumed if necessary, and shall end. It shall mention the identity of the persons who intervene at the hearing or at any part thereof. At the end of the hearing, the person questioned shall have the right to read it again or to request that it be read to him. It may request that its declarations be corrected or completed. The staff members of the inspection service who interview a person shall inform the person that he or she may request a copy of the text of the hearing. This copy shall be issued free of charge.

§ 6. The members of the inspection service may consult all the information media and the data they contain. They may obtain on the spot the computer system and the data contained therein which they need for their examinations and findings, and take or request extracts, duplicates or copies free of charge, in a legible and intelligible form which they have requested. If it is not possible to take copies on the spot, the members of the inspection service may seize the computer system and the data contained therein against a receipt containing an inventory.

§ 7. In order to extend a search of a computer system or part thereof initiated on the basis of paragraph 6 to a computer system or part thereof in a location other than that in which the search is being conducted, the inspection service may request the intervention of an investigating judge.

Art. 45.

§ 1. After each inspection, the members of the inspection service shall draw up a report and send a copy to the inspected operator of essential services and to the competent sectoral authority.

§ 2. The authority referred to in Article 7(1) and the sectoral authority may request the inspection service to forward its inspection reports, giving reasons.

Art. 46.

§ 1. The essential services operator shall cooperate fully with the members of the inspection service in the performance of their duties and in particular to inform them as fully as possible of all existing security measures. If necessary, the operator of essential services shall provide the members of the inspection service or the sectoral authority with the necessary equipment so that they can fulfil the safety instructions during inspections.

§ 2. The King may determine, by sector or sub-sector, by order deliberated in the Council of Ministers and after the opinion of the sectoral authority, fees for inspection services. These fees are charged to the operators of essential services.

It sets out the calculation and payment procedures.

CHAPTER 2. - Control of digital service providers

Art. 47.

§ 1. The King shall lay down the practical arrangements for the supervision of digital service providers.

§ 2. The digital service provider is required to, inter alia:

a) provide, within the required time, to the relevant inspection body the information necessary to assess the security of its networks and information systems, including documents relating to its security policies;

b) to correct any breach of security and incident reporting requirements within the required timeframe.

§ 3.

In accordance with the rules laid down by the King, the inspection service may adopt measures, if necessary, in the context of ex post control measures, when, according to the elements communicated, a digital service provider does not meet the security or incident reporting requirements. These elements may be communicated by a competent authority of another Member State of the European Union where the service is provided.

§ 4.

In the framework of its post-checks, the inspection service shall have the same powers as those provided for in Article 44.

§ 5.

If a digital service provider has its principal place of business or a representative in Belgium but its networks and information systems are located in one or more other States, the inspection service, in consultation with the authority referred to in Article 7, § 1, may request the cooperation and assistance of the competent supervisory authorities of those other States. Such assistance and cooperation may include exchanges of information and requests for enforcement action.

§ 6.

In accordance with the rules laid down by the King, the inspection service may also exercise the powers provided for in this Article at the request of the competent authorities of another Member State of the European Union.

§ 7.

The authority referred to in Article 7(1) may request the inspection service to forward the inspection reports of a digital service provider.

§ 8.

The King may determine, by decree deliberated in the Council of Ministers and after the opinion of the sectoral authority, fees for inspection services. These fees are charged to the digital service providers. The King shall determine the manner of calculation and payment.

CHAPTER 3. - Penalties Section 1. - Procedure

Art. 48.

§ 1. Where one or more breaches of the requirements imposed by the law, its implementing decrees or the individual administrative decisions relating thereto are found, the inspection service shall give formal notice to the operator of essential services or digital service provider concerned to comply with the obligations incumbent upon it within a period to be determined by the inspection service.

The time limit shall be determined taking into account the operating conditions of the operator of essential services or digital service provider and the measures to be implemented.

§ 2. Before doing so, the inspection service shall inform the offender, giving reasons, of its intention to issue a letter of formal notice and shall inform him of his right, within 15 days of receiving this information, to put forward his defence in writing or to request a hearing. The information is presumed to have been received

by the offender on the sixth day after it is sent by the inspection service.

§ 3. On the basis of the information in its possession, the authority referred to in Article 7(1) may also recommend to the inspection service that it give formal notice to the operator of essential services or the digital service provider, giving reasons.

Art. 49.

§ 1. Where the inspection service finds that the operator of essential services or digital service provider has not complied with the formal notice within the time limit set, the facts shall be recorded in a report drawn up by the sworn members of the inspection service. This report shall be sent to the competent sectoral authority.

§ 2. Any person who deliberately prevents or hinders the carrying out of an inspection by members of the inspection service, refuses to communicate information requested in connection with the inspection, or knowingly communicates incorrect or incomplete information shall be recorded in a report by the sworn members of the inspection service.

§ 3. Paragraphs 1 and 2 shall also apply to a potential operator of essential services or operator of critical infrastructure who fails to comply with the information obligations referred to in Article 14 or Article 18(3).

§ 4. The minutes drawn up by the sworn members of the inspection service are authentic until proven otherwise.

Art. 50.

Violations of this Law or its implementing acts may be subject to either criminal or administrative sanctions.

Section 2. - Criminal penalties

Art. 51.

§ 1. Any person who fails to comply with any of the incident reporting obligations referred to in Articles 24 or 35 shall be punished by imprisonment for a term of eight days to one year and a fine of EUR 26 to EUR 20 000 or by one of these penalties only.

§ 2. Any person who fails to comply with any of the security obligations imposed by the King or the sectoral authority under section 21 or 33 shall be punished by imprisonment for a term of eight days to one year and a fine of 26 euros to 30,000 euros or by one of these penalties only.

§ 3. Any person who fails to comply with any of the control obligations referred to in Chapters 1 and 2 of Title 4 shall be liable to imprisonment for a term of eight days to one year and a fine of EUR 26 to EUR 50 000, or to both.

§ 4. Any person who fails to comply with any of the information obligations referred to in Article 14 or Article 18 § 3 shall be punished by imprisonment for a term of eight days to one year and a fine of 26 euros to 50,000 euros or by one of these penalties only.

§ 5. Any person who wilfully prevents or hinders the performance of an inspection by members of the inspection service, refuses to provide information requested in connection with the inspection, or knowingly provides inaccurate or incomplete information, shall be punished by imprisonment for a period of eight days to two years and a fine of 26 euros to 75,000 euros, or by one of these penalties only.

§ 6. In the event of a repeat offence for the same acts within a period of three years, the fine is doubled, and the offender is punished by a prison sentence of fifteen days to three years.

§ 7. The provisions of Book 1 of the Criminal Code, including Chapter VII and Article 85, shall apply to the offences referred to in this Article. Articles 269 to 274 and 276 of the Criminal Code apply to members of the inspection service acting in the performance of their duties.

§ 8. Violations of Article 9, §§ 2 and 3 of this Act shall be punishable by the penalties provided for in Article 458 of the Penal Code.

Section 3. - Administrative penalties

Art. 52.

§ 1. An administrative penalty may be imposed for any violation of this Law, its implementing orders or administrative decisions taken pursuant to this Law.

§ 2. A fine of EUR 500 to EUR 75 000 shall be imposed on any person who fails to comply with the incident reporting obligations referred to in Articles 24 or 35.

§ 3. Any person who fails to comply with the security obligations imposed by the King or the sectoral authority pursuant to Article 21 or 33 shall be liable to a fine of between 500 and 100,000 euros.

§ 4. Any person who fails to comply with the information obligations referred to in Article 14 or Article 18(3) shall be liable to a fine of between 500 and 125 000 euros.

§ 5. Any person who fails to comply with the control obligations referred to in Chapters 1 and 2 of Title 4 shall be liable to a fine of EUR 500 to EUR 200 000.

§ 6. A fine of between EUR 500 and EUR 200,000 shall be imposed on anyone who causes a person acting on behalf of an operator of essential services or digital service provider to suffer adverse consequences as a result of performing, in good faith and within the scope of his duties, the obligations arising from this Act.

Art. 53. The original of the report is sent by the inspection service to the public prosecutor. A copy of the report is sent to the offender at the same time.

Art. 54. The public prosecutor has two months from the day of receipt of the report to inform the sectoral authority that criminal proceedings have been initiated. The sectoral authority may not initiate the procedure for imposing an administrative fine before the expiry of the aforementioned time limit, unless the Public Prosecutor has previously communicated that he or she does not wish to follow up the matter. In the event that the public prosecutor fails to notify his or her decision within the set time limit or refrains from instituting criminal proceedings, the sectoral authority may decide to initiate the administrative procedure.

Art. 55.

§ 1. Reasons shall be given for the decision to impose an administrative fine. It shall also state the amount of the administrative fine and the infringements concerned.

§ 2. The sectoral authority shall inform the offender in advance of its reasoned proposal for an administrative penalty and shall inform him of his right, within fifteen days of receiving the proposal, to put forward his defence in writing or to request a hearing. The proposal is presumed to have been received by the offender on the sixth day after it is sent by the sectoral authority.

§ 3. Taking into account the defences raised within the time limit referred to in paragraph 2 or in the absence of a reaction from the offender within the same time limit, the sectoral authority may adopt an administrative penalty referred to in Article 52.

§ 4. The administrative fine is proportional to the seriousness, duration, means used, damage caused and circumstances of the facts. The administrative fine is doubled in the event of a repeat offence for the same acts within a period of three years.

§ 5. A combination of several offences may give rise to a single administrative fine proportionate to the seriousness of the offences as a whole.

Art. 56.

The decision is notified to the offender by registered mail. An invitation to pay the fine within one month is attached to the decision.

Art. 57.

The offender may challenge the decision of the sectoral authority before the Market Court referred to in Article 101 of the Judicial Code. The application shall be made by means of an application in which both parties are heard and shall be submitted within sixty days of notification of the decision of the sectoral authority, failing which it shall lapse. The case shall be dealt with in the form of summary proceedings in accordance with Articles 1035 to 1038, 1040 and 1041 of the Judicial Code. This appeal does not suspend the execution of the decision.

Art. 58.

§ 1. If the offender fails to pay the administrative fine within the time limit, the decision to impose an administrative fine is enforceable and the sectoral authority may issue a constraint. The constraint is issued by the legal representative of the sectoral authority or by a member of staff authorised for this purpose.

§ 2. The constraint is served to the offender by a bailiff's writ. The notification shall contain an order to pay within twenty-four hours, under penalty of execution by way of seizure, as well as an accounting justification of the sums demanded and a copy of the writ of execution.

§ 3. The offender may lodge an objection to the constraint before the seizure judge. Reasons shall be given for the objection, failing which it shall be null and void. It shall be made by means of a summons to the sectoral authority by bailiff's writ within fifteen days of the service of the constraint. The provisions of Chapter VIII of Part I of the Judicial Code shall apply to this period, including the extensions provided for in Article 50, paragraph 2, and Article 55 of the Code. The opposition to the constraint shall suspend the enforcement of the constraint, as well as the prescription of the claims contained in the constraint, until a decision has been taken on its merits. Seizures already carried out previously shall retain their conservatory character.

§ 4. The sectoral authority may order the precautionary seizure and enforce the constraint by means of the enforcement procedures provided for in Part V of the Judicial Code. Partial payments made following the service of a constraint shall not prevent the continuation of proceedings.

§ 5. The costs of serving the constraint as well as the costs of enforcement or precautionary measures shall be borne by the offender. They shall be determined in accordance with the rules established for acts performed by judicial officers in civil and commercial matters.

Art. 59. The sectoral authority may not impose an administrative fine after a period of three years from the day on which the act was committed. Payment under the administrative procedure also extinguishes the possibility of criminal prosecution for the acts in question.

TITLE 5. - CSIRT

CHAPTER 1. - The National CSIRT

Section 1. - Tasks of the National CSIRT

Art. 60.

The tasks of the national CSIRT are at least the following:

a) the monitoring of incidents at national and international level, including the processing of personal data related to the monitoring of such incidents;

b) activation of the early warning mechanism, dissemination of warning messages, announcements and

dissemination of information on risks and incidents to interested parties;

c) incident response;

d) dynamic risk and incident analysis and situational awareness;

e) detection, observation and analysis of computer security problems;

f) promoting the adoption and use of common or standardised practices for risk and incident management procedures, as well as incident, risk and information classification systems;

g) the establishment of cooperative relationships with the private sector, other administrative services or public authorities;

h) participation in the CSIRT network referred to in Article 12 of the NIS Directive. The King may, on the advice of the national CSIRT, assign additional tasks to it.

Section 2. - Obligations of the National CSIRT

Art. 61.

The obligations of the national CSIRT are at least the following:

a) ensure a high level of availability of its communication services by avoiding single points of failure and having multiple ways to be contacted and to contact others at any time;

b) have premises and information systems located on secure sites;

c) ensure continuity of operations with an appropriate request management and routing system to facilitate transfers;

d) participate in meetings of the CSIRT network referred to in Article 12 of the NIS Directive;

e) rely on an infrastructure with guaranteed continuity. For this purpose, redundant systems and a backup workspace are available;

f) ensure that its communication channels are clearly specified and well known to its partners.

Art. 62. In exercising its powers, the national CSIRT shall take all appropriate measures to achieve the objectives set out in Articles 60 and 61. These measures must be proportionate to these objectives and respect the principles of objectivity, transparency and non-discrimination. To achieve these objectives, the National CSIRT is authorized to hold, disclose to another person, disseminate, or make use of all available information, even if it is derived from unauthorized access to a computer system by a third party. In the performance of its duties, the National CSIRT shall exercise the care that may be expected of a public authority, always giving priority to avoiding disruption of the computer system and taking all reasonable precautions to ensure that no material damage is caused to the computer system. The senior officials of the national CSIRT shall ensure, through the adoption of internal procedures, that the conditions referred to in this Article are met.

CHAPTER 2. - The sectoral CSIRT

Section 1. - Tasks of the sectoral CSIRT

Art. 63.

The tasks of a sectoral CSIRT are, in collaboration with the national CSIRT, at least the following:

a) monitoring of sectoral incidents;

b) activation of the early warning mechanism, dissemination of warning messages, announcements and dissemination of information on risks and incidents to industry stakeholders;

c) sector incident response;

d) dynamic analysis of sectoral risks and incidents and situational awareness;

e) establishing cooperative relationships with operators in its sector;

f) be able to participate in the meetings of the CSIRT network referred to in Article 12 of the NIS Directive that are relevant to their sector. The King may, after consultation with the sectoral CSIRT, assign additional tasks to it.

Section 2. - Obligations of a sectoral CSIRT

Art. 64.

The obligations of a sectoral CSIRT are as follows:

a) ensure a high level of availability of its communication channels by avoiding single points of failure and having several ways to be contacted and to contact others at any time.

b) have premises and information systems located on secure sites.

c) ensure continuity of operations with an appropriate request management and routing system to facilitate transfers.

d) rely on an infrastructure with guaranteed continuity. Redundant systems and a backup workspace are available for this purpose.

f) ensure that its communication channels are clearly specified and well known to its partners. TITLE 6.
- Processing of personal data

CHAPTER 1. - Principles of processing, legal basis and purposes

Art. 65.

§ 1. In accordance with Article 5(1)(c) of the EU Regulation 2016/679, when processing personal data in the context of the execution of this Act, the controller shall ensure that the processing is limited to the minimum necessary and proportionate to the purpose.

§ 2. In compliance with this principle, the personal data processed may be data of any type relating to the security of networks and information systems, namely, where applicable, personal information, data concerning an organisation's employees or external persons, connection data or identifiers, geolocation data, identification or authentication data, where applicable by means of secure devices.

§ 3. The main processing of personal data under this Act can be grouped as follows: - the general exchange of information between operator of essential services and digital service providers on the one hand and the authorities referred to in Article 7 on the other hand; - the processing of specific information between the entities referred to in the first indent in the context of incident notifications or other ad hoc exchanges; - the processing by the inspection services in accordance with Title 4; - processing by the courts and tribunals or the sectoral authorities in the context of the implementation of the law and in particular the investigation, prosecution and punishment of offences; - exchanges and other processing of information by the national CSIRT and by the sectoral CSIRT for their tasks referred to in Articles 60 to 62 and 63 and 64 respectively.

Art. 66.

§ 1. Wherever possible, the data processed is pseudonymised or aggregated so as to reduce the risk of

personal data being used in a way that is incompatible with EU Regulation 2016/679 or the laws and regulations that supplement or specify it.

§ 2. Special categories of data within the meaning of Articles 9 and 10 of the EU Regulation 2016/679 shall be processed in compliance with the said Regulation and the laws and regulations that supplement or specify it.

§ 3. The controller may be either one of the authorities referred to in Article 7, operators of essential services or digital service providers, or police or judicial authorities.

§ 4. The recipients of personal data may be all persons involved in the execution of the provisions of the law, to the extent necessary for the exchange of information provided for by the law.

Art. 67.

According to Articles 6.1(c) and 6.1(e) of the EU Regulation 2016/679, the processing operations referred to in Article 65(3) must remain necessary for compliance with a legal obligation of the controller or for the performance of a task carried out in the public interest by the controller. Such processing must be necessary for these legal purposes only and must be limited to what is necessary to fulfil them.

Art. 68.

§ 1. The processing operations referred to in Article 65(3) must be limited to and remain compatible with the purposes determined by the controller.

§ 2. These purposes may include the search for an increased level of protection of networks and information systems, the reinforcement of prevention and security policies, the prevention of security incidents, the continuity of essential services or digital services covered by this law, the control of operator of essential services and digital service providers, cooperation at national and international level, the evaluation of the implementation of the law, the preparation, organisation, management and follow-up of investigations or prosecutions, as well as the other tasks devolved by law to the various authorities concerned.

§ 3. It is for each controller to determine the relevant purposes or sub-purposes, the categories of data and data subjects, the recipients or categories of recipients of the data, the retention periods and any other characteristics of the processing operation, as well as the rules and practices for compliance with the applicable regulations.

CHAPTER 2. - Retention period

Art. 69.

§ 1. Without prejudice to the retention necessary for processing for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes, referred to in Article 89 of the EU Regulation 2016/679, personal data processed in execution of the law, shall not be kept by the authorities referred to in Article 7 longer than necessary with regard to the purposes for which they are processed.

§ 2. In compliance with paragraph 1, the King may set the maximum period of retention of the same data by decree deliberated in the Council of Ministers.

CHAPTER 3. - Data Protection Officer

Art. 70. Any operator of essential services, any digital service provider and any authority referred to in Article 7 of the Act that processes personal data shall appoint a data protection officer.

CHAPTER 4 - Limitation of data subjects' rights

Art. 71.

§ 1. Pursuant to Articles 23.1(a), (b), (c), (d), (e), (h), of the EU Regulation 2016/679, certain obligations and rights provided for in that Regulation are limited or excluded, in accordance with the provisions of this Chapter. Such limitations or exclusions may not prejudice the essence of the fundamental rights and freedoms and must be applied to the extent strictly necessary for the purpose.

§ 2. Articles 12 to 22 of the said Regulation shall not apply to the processing of personal data by an operator of essential services, a digital service provider or an authority referred to in Article 7, which is carried out in compliance with this Act and in order to fulfil the obligations it imposes with regard to the incident notifications referred to in Chapter 3 of Title 2 and Chapter 3 of Title 3, as well as the checks referred to in Title 4. The exemption shall apply only if and insofar as such processing is necessary for the purposes defined above, in particular insofar as the application of the rights provided for in the abovementioned Regulation would be detrimental to the needs of the control, investigation or preparatory acts, or would risk violating the confidentiality of the criminal investigation or the safety of individuals.

§ 3. The controller who may benefit from the exemption provided for in paragraph 2 shall be either the operator of essential services, the digital service provider or the authority referred to in Article 7, each in respect of the data held in the context of the tasks referred to in paragraph 2.

§ 4. The exemption shall apply, subject to the principle of proportionality and, where appropriate, data minimisation, to all categories of personal data insofar as the processing of such data is not unrelated to the purposes referred to in paragraph 2. This exemption shall also apply to preparatory acts or to procedures for the possible application of an administrative penalty.

§ 5. Personal data resulting from the exemption referred to in paragraph 2 shall be kept for no longer than is necessary for the purposes for which they are processed, and for no longer than the limitation period for any offences referred to in Articles 51 and 52, in accordance with the applicable law.

§ 6. A data controller who does not comply with all the provisions of the Act, and in particular Article 72, cannot benefit from the exemption.

§ 7. Each data controller is also obliged to maintain the confidentiality of the personal data that are the subject of the exemption, and to ensure that they are accessible only to those persons who need them for the execution of the provisions of this law. Each controller concerned must also send to the Data Protection Authority, at least once a year, a written list of requests for the exercise of the rights referred to in Articles 12 to 22 of the Regulation which, according to the controller, fall within the scope of the exemption. Without prejudice to the provisions of this Act, each data controller concerned is furthermore required to take any other appropriate measures to prevent any form of unlawful abuse, access or transfer of personal data that falls within the scope of the exemption, namely and without any limitation whatsoever the measures provided for in Article 32 of the EU Regulation 2016/679.

Art. 72.

§ 1. Data subjects may send a request regarding their rights under Articles 12 to 22 of the EU Regulation 2016/679, to the Data Protection Officer, who shall acknowledge receipt.

§ 2. The Data Protection Officer of the controller shall inform the data subject in writing as soon as possible, and in any event within one month of receipt of the request, of any refusal or restriction of his or her rights under Articles 12 to 22 of Regulation EU 2016/679, and of the reasons for the refusal or restriction. Such information concerning refusal or restriction may be withheld where its disclosure would jeopardise one of the purposes set out in Article 71(2). If necessary, this period may be extended by two months, taking into account the complexity and number of requests.

The controller shall inform the data subject of this extension and the reasons for the postponement within one month of receipt of the request.

§ 3. The Data Protection Officer of the data controller shall inform the data subject of the possibilities to lodge a complaint with the Data Protection Authority and to seek judicial remedy. The Data Protection Officer of the data controller shall record the factual or legal grounds on which the decision is based. This information shall be made available to the Data Protection Authority.

§ 4. However, the data controller concerned shall provide the data subject with access to limited information concerning the processing of his/her personal data, provided that such communication does not jeopardise the attainment of the objectives of this Act and in such a way that the data subject is unable to ascertain whether he/she is being investigated or not, and without being able to rectify, erase, restrict, notify, transmit to a third party or cease any form of processing of the said data that is necessary within the framework defined above.

§ 5. The measure of refusal or limitation of rights provided for in Articles 12 to 22 of Regulation EU 2016/679, must be lifted: - for measures justified by the incident reporting obligations, upon closure of the processing of an incident by the authorities referred to in Article 24 or 34; - for measures justified by the obligations under Title 4, upon closure of the inspection or investigation or preparatory acts thereto carried out by the inspection service, as well as during the period in which the sectoral authority is processing the material from the inspection service with a view to prosecution; - at the latest one year from the receipt of the request made pursuant to Articles 12 to 22 of the EU Regulation 2016/679, unless an inspection or investigation is in progress.

§ 6. The controller concerned shall also lift the measure of refusal or restriction of rights provided for in Articles 12 to 22 of Regulation EU 2016/679, as soon as such a measure is no longer necessary for compliance with one of the purposes referred to in Article 68, § 2.

§ 7. In all cases of application of paragraphs 5 and 6, the Data Protection Officer shall inform the data subject(s) in writing of the lifting of the refusal or restriction.

CHAPTER 5. - Limitations to the obligations to notify personal data breaches

Art. 73.

The controller concerned shall be exempted from notifying a personal data breach to a specific data subject or data subjects, as defined in Article 34 of Regulation EU 2016/679, subject to the authorisation of the authority referred to in Article 7(1), provided that and to the extent that such individual notification is likely to jeopardise the purposes referred to in Article 71(2).

TITLE 7. - Final provisions

CHAPTER 1. - Amendments to the Act of 1 July 2011 on the security and protection of critical infrastructure

Art. 74.

Article 2 of the Act of 1 July 2011 on the security and protection of critical infrastructures is supplemented by a paragraph worded as follows: "This Act partially transposes 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 security of networks and information systems in the Union."

Art. 75.

In section 3 of the same Act, as amended by the Acts of 25 April 2014 and 15 July 2018, the following amendments are made:

1° in 3°, c) and d) are replaced by the following: "(c) for the financial sector, with the exception of trading platform operators within the meaning of Article 3, 6°, of the Law of 21 November 2017 on infrastructures for markets in financial instruments and transposing Directive 2014/65/EU: The National Bank of Belgium (NBB);

d) for trading platform operators within the meaning of Article 3, 6°, of the Law of 21 November 2017 on infrastructures for markets in financial instruments and transposing Directive 2014/65/EU: The Financial Services and Markets Authority (FSMA);"; 2° 3° is completed by e) to g) drafted as follows: **e)** for the electronic communications and digital infrastructure sectors: the Belgian Institute for Postal Services and Telecommunications (I.B.P.T.);

f) for the health sector: the public authority designated by the King by order deliberated in the Council of Ministers;

g) for the drinking water sector: the public authority designated by the King by order deliberated in the Council of Ministers;";

3) the article is completed by 13° to 17° drafted as follows: - "13° "the Act of 7 April 2019": The Act of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security;

- 14° "security of networks and information systems" means the security of networks and information systems within the meaning of Article 6, 8° and 9° of the Law of 7 April 2019;

- 15° "the digital infrastructure sector" means the sector referred to in point 6 of Annex 1 to the Law of 7 April 2019;

- 16° "the drinking water sector": the sector referred to in point 5 of Annex 1 to the law of 7 April 2019; - 17° "the health sector": the sector referred to in point 4 of Annex 1 to the law of 7 April 2019."

Art. 76.

In section 4 of the Act, as amended by the Act of July 15, 2018, paragraph 4 is replaced by the following: " § 4. This Chapter shall apply to the financial sector, including the trading platform operators referred to in Article 3(3)(d), the electronic communications sector, the digital infrastructure sector, the health sector and the drinking water sector, as regards the security and protection of national critical infrastructure.

Art. 77.

Section 5 of the same Act, as amended by the Act of July 15, 2018, shall be supplemented by subsection 3, which shall read as follows: " § 3. Throughout the identification process referred to in this section, the authority referred to in Article 7, § 1, of the Act of 7 April 2019 shall be involved in the national and international consultations conducted by the sectoral authorities and the DGCC, for the aspects of the identification of critical infrastructures related to the security of networks and information systems."

Art. 78.

In section 13 of the same Act, as amended by the Acts of 25 April 2014 and 15 July 2018, the following amendments are made:

1) in paragraph 5a, the words "with the exception of those operated by a trading platform operator" are inserted between the words "of the financial sector" and the words ", security measures".

2) in the first subparagraph of paragraph 6, the words "with the exception of critical infrastructures operated by a trading platform operator" are inserted between the words "the financial sector" and the words ",

financial years".

Art. 79.

In Article 14 of the same Act, as amended by the Act of 15 July 2018, the words "and, where appropriate, the authority referred to in Article 7, § 1, of the Act of 7 April 2019, as regards the security of networks and information systems," shall be added to paragraph 2.

Art. 80.

In Article 18 of the same Act, as amended by the Act of 15 July 2018, the words "The DGCC, the police services and the OCAM" are replaced by the words "The DGCC, the police services, the OCAM and, where appropriate, the authority referred to in Article 7, § 1, of the Act of 7 April 2019 as regards the security of networks and information systems".

Art. 81.

In Article 19 of the same Act, the words "The operator, the security contact point, the sectoral authority, the DGCC, the OCAM and the police services" are replaced by the words "The operator, the security contact point, the sectoral authority, the DGCC, the OCAM, the police services and, where applicable, the authority referred to in Article 7(1) of the Act of 7 April 2019 with regard to the security of networks and information systems".

Art. 82.

In Article 22 of the same Act, replaced by the Act of 15 July 2018, the words "The sectoral authority, the DGCC, the OCAM and the police services" shall be replaced by: "The sectoral authority, the DGCC, the OCAM, the police services and the authority referred to in Article 7, § 1, of the Law of 7 April 2019,".

Art. 83.

In Article 22bis of the same law, inserted by the law of 25 April 20048 , the following amendments are made: 1° in paragraph 1, the words "with the exception of the sub-sector of trading platform operators" are inserted between the words "the financial sector" and the words ", the National Bank of Belgium".2° a paragraph is added to the article as follows: "For trading platform operators, FSMA shall provide the Minister of Finance with a report on the tasks it performs under this law at appropriate intervals not exceeding three years. However, FSMA shall inform it without delay of any concrete and imminent threat to a critical infrastructure within its sector.

Art. 84.

In section 24 of the same Act, as amended by the Acts of 25 April 2014 and 15 July 2018, the following amendments are made:

1° in paragraph 2, subparagraph 3, the words "with the exception of the sub-sector of trading platform operators" are inserted between the words "the financial sector" and the words ", the National Bank of Belgium".

2° a subparagraph is added to paragraph 2 as follows: "The Authority for Financial Services and Markets is designated as the inspection service responsible for monitoring the application of the provisions of this Law and its implementing decrees, for trading platform operators within the meaning of Article 3, 6°, of the Law of 21 November 2017 on the infrastructure of markets in financial instruments and transposing Directive 2014/65/ EU. This Article shall not prejudice the possibility for FSMA, in order to carry out the tasks entrusted to it by this law, to entrust an external specialised service provider with the performance of specific tasks or to obtain the assistance of such a service provider.

CHAPTER 2. - Amendments to the law of 15 April 1994 on the protection of the population and the environment against the dangers resulting from ionising radiation and on the Federal Agency for Nuclear Control

Art. 85.

Article 1 of the Act of 15 April 1994 on the protection of the population and the environment against the dangers resulting from ionising radiation and on the Federal Nuclear Control Agency, as last amended by the Act of 13 December 2017, is supplemented as follows: - "the Act of 7 April 2019": The Act of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security;".

Art. 86.

In Section 1 of Chapter III of the same Act, the following article 15ter is inserted "Art. 15ter. The Agency is designated as an inspection service, within the meaning of Article 42 of the Act of 7 April 2019 and is responsible for monitoring the application of the provisions of the said Act and its implementing decrees by the operators of essential services, identified under the aforementioned Act, with regard to the components of a nuclear installation intended for the industrial production of electricity and which are used for the transmission of electricity.

The King shall lay down the practical arrangements for the inspections, after obtaining the opinion of the Agency.".

CHAPTER 3. - Amendments to the Act of 17 January 20037 on the status of the regulator of the Belgian postal and telecommunications sectors

Art. 87.

Article 1/1 of the Act of 17 January 20037 on the status of the regulator of the Belgian postal and telecommunications sectors, inserted by the Act of 10 July 2012, is supplemented by the following paragraph: "This Act partially transposes 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 security of networks and information systems in the Union."

Art. 88.

In Article 14, § 1, paragraph 1, of the same Act, as amended by the Acts of 13 December 2010, 10 July 2012, 27 March 2014, 18 April 2017, 5 May 2017 and 31 July 2017, the following amendments are made:

1) in paragraph 1, the words ", as regards the digital infrastructure sector within the meaning of the Act of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security, as regards the electronic communications and digital infrastructure sectors within the meaning of the Act of 1 July 2011 on the security and protection of critical infrastructures," are inserted between the words "radio equipment" and the words "and as regards";

2) paragraph 3 is replaced by the following "3) monitoring compliance with the following standards and their implementing orders:

a) the law of 13 June 20052 on electronic communications;

b) Title I, Chapter X and Title III of the Law of 21 March 1991 on the reform of certain economic public enterprises;

c) the postal services act of 26 January 2018;

d) Articles 14(2)(2) and 21(5) to (7) of the Act of 17 January 20037 on the status of the regulator of the

Belgian postal and telecommunications sectors;

e) Articles 4 and 4/1 of the Law of 17 January 20037 concerning appeals and the handling of disputes in connection with the Law of 17 January 20037 on the status of the regulator of the Belgian postal and telecommunications sectors;

f) the law of 5 May 2017 on audio-visual media services in the bilingual region of Brussels-Capital;

g) the law of 1 July 2011 on the security and protection of critical infrastructures, as regards the electronic communications and digital infrastructures sectors;

h) the Act of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security, as regards the digital infrastructure sector;

i) Commission Regulation (EU) 611/2013 of 24 June 2013 on measures concerning the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications. For the application of the Act of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security, the Institute is designated as the sectoral authority and inspection service for the digital infrastructure sector. The King may lay down the practical arrangements for inspections in this sector, after consulting the Institute.

Art. 89.

In Article 24, paragraph 1, of the same Act, as amended by the Acts of 27 March 2014 and 26 January 2018, the words ", as well as to the Act of 1 July 2011 on the security and protection of critical infrastructures, as regards the electronic communications sector and the digital infrastructures sector, and the Law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security, as regards the digital infrastructure sector," are inserted between the words "in the bilingual region of Brussels-Capital" and the words "and their implementing decrees".

CHAPTER 4. - Amendments to the Law of 21 November 2017 on market infrastructures for financial instruments and transposing Directive 2014/65/EU

Art. 90.

The words "and Title 2 of the Act of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security" shall be added to Article 71 of the Act of 21 November 2017 on the infrastructures of financial instruments markets and transposing Directive 2014/65/EU. In order to carry out the aforementioned tasks relating to the Act of 7 April 2019, the FSMA may, however, entrust a specialised external service provider with the performance of specific supervisory tasks or obtain the assistance of such a service provider. ".

Art. 91.

Article 79 of the same law is supplemented by a paragraph 4, which reads as follows: " § 4. In the event of violation of the applicable provisions of the Law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security, FSMA may impose the administrative sanctions provided for in Article 52 of the said Law."

CHAPTER 5. - Amendment of the Act of 2 August 20026 on the supervision of the financial sector and on financial services

Art. 92.

Article 75, § 1, 15°, of the Law of 2 August 20026 on the supervision of the financial sector and on financial services, repealed by the Law of 5 December 2017 on various financial provisions, is reinstated in the following wording: "15° within the limits of European Union law, the authorities referred to in Article 7 of the Act of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security for the purposes of implementing the provisions of that Act and the Act of 1 July 2011 on the security and protection of critical infrastructures;"

CHAPTER 6 - Amendments to the Law of 22 February 1998 laying down the Organic Statute of the National Bank of Belgium

Art. 93. Article 36/1 of the Law of 22 February 1998 laying down the Organic Statute of the National Bank of Belgium, inserted by the Royal Decree of 3 March 2011, is supplemented by 28° worded as follows: "28) "the Act of 7 April 2019" means the Act of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security."

Art. 94. In Article 36/14, § 1, of the same Act, as last amended by the Act of 30 July 2018, the following amendments are made:

1° in 20° the words "to the authority referred to in Article 7, § 1, of the Act of 7 April 2019"; inserted between the words "the threat analysis" and "and to the police services";

2° the paragraph is completed by 24°, which reads as follows "24° within the limits of European Union law, to the authorities referred to in Article 7 of the Act of 7 April 2019 for the purposes of implementing the provisions of the Act of 7 April 2019 and the Act of 1 July 2011 on the security and protection of critical infrastructures."

Art. 95. In the same law, a Chapter IV/4 is inserted, with Article 36/47, which reads as follows "Chapter IV/4. Monitoring by the Bank under the Act of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security.

Art. 36/47. "For the application of the law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security, the Bank is designated as sector authority and inspection service for operators in the finance sector, with the exception of trading platform operators within the meaning of Article 3, 6°, of the law of 21 November 2017 on the infrastructures of the markets in financial instruments and transposing Directive 2014/65/EU. Articles 36/19 and 36/20 shall apply. The Sanction Commission shall decide on the imposition of the administrative fines provided for in Article 52 of the aforementioned Act of 7 April 2019. Articles 36/8 to 36/12/3 and article 36/21 shall apply. The Bank shall share with the ECB as soon as possible relevant information on incident notifications it receives under the Act of 7 April 2019."

CHAPTER 7. - Entry into force

Art. 96. This law enters into force on the day of its publication in the Moniteur belge.

Art. N1. Annex 1 Types of operator of essential services referred to in Article 11(1)

Sector	Sub-sector	Type of entities
1. Energy	a) Electricity	Electricity companies within the meaning of Article 2, 15°ter of the Law of 29 April 1999 on the organisation of the electricity market. Distribution system operators within the meaning of Article 2, 11° of the Law of 29 April 1999 on the organisation of the electricity market. Network operators within the meaning of Article 2, 8° of the Law of 29 April 1999 on the organisation of the electricity market.
	b) Oil	Pipeline operators. Operators of oil production, refining, processing, storage and transportation facilities.
	c) Gas	Natural gas companies within the meaning of Article 1, 5° bis of the Law of 12 April 1965 on the transport of gaseous and other products through pipelines. Distribution network operators within the meaning of Article 1, 13° of the Law of 12 April 1965 on the transport of gaseous and other products through pipelines. Operators of the natural gas transmission system within the meaning of Article 1, 31° of the Law of 12 April 1965 on the transmission of gaseous and other products by pipeline. Storage operators within the meaning of Article 1, 33° of the Law of 12 April 1965 on the transport of gaseous and other products by pipeline. Managers of LNG installations within the meaning of Article 1, 35° of the Law of 12 April 1965 on the transport of gaseous and other products by pipeline. Operators of natural gas refining and processing facilities.
2. Transportation	a) Air transport	Air carriers as defined in 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(2) of the Royal Decree of 6 November 2010 regulating access to the ground handling market at Brussels Airport, airports within the meaning of Article 2(1) of Directive 2009/12/EC of the European Parliament and of the Council, including core network airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council, and entities operating ancillary facilities located at

		airports. Air navigation services within the meaning of Article 2(4) 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 ("framework regulation"). The network operator within the meaning of Article 2(22) of Commission Regulation (EU) No 677/2011 of 7 July 2011 laying down detailed rules for the performance of air traffic management network functions and amending Regulation (EU) No 691/2010.
	b) Rail transport	Infrastructure managers within the meaning of Article 3, 29° of the Railway Code. Railway undertakings within the meaning of Article 3, 27° of the Railway Code.
	c) Transport by water	Land, sea and coastal passenger and freight transport companies as defined in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council, excluding ships operated individually by these companies. Entities managing ports within the meaning of Article 5(7) of the Act of 5 February 2007 on maritime 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 the ports Vessel traffic service operators (VTS) within the meaning of Article 1(12) of the Royal Decree of 17 September 2005 implementing Directive 2002/59/EC of 27 June 2002.
	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 with regard to the provision of real-time traffic information services throughout the Union, responsible for traffic management control. Operators of intelligent transport systems within the meaning of Article 3(1) of the Act of 17 August 2013 establishing the framework for the deployment of intelligent transport systems and amending the Act of 10 April 1990 regulating private and particular security (hereinafter referred to as the "ITS Framework Act").
3. Finance	a) Financial institutions	Credit institutions as defined in Article 4(1) of 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 648/2012. 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. Financial institutions (other than credit institutions and central counterparties) subject to supervision by the National Bank of Belgium, pursuant to Articles 8 and 12a of the Law of 22 February 1998 laying down the Organic Statute of the National Bank of Belgium.
	b) Financial trading platforms	Trading platform operators within the meaning of Article 3, 6° of the Law of 21 November 2017 on infrastructures for markets in financial instruments and transposing Directive 2014/65/EU.
4. Health	Health care facilities (including hospitals and private clinics)	Healthcare providers as defined in Article 3(g) of 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.
5. Drinking water		Suppliers and distributors of water intended for human consumption within the meaning of Article 2(1)(a) of Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption, excluding distributors for whom the distribution of water intended for human consumption is only part of their general activity of distributing other products and goods which are not considered essential services.
6. digital infrastructure		IXP. DNS service providers. Top level domain name registries.

Art. N2. Annex 2 Types of digital services

1. Online marketplace
2. Online search engines
3. Cloud computing service