EnCaViBS

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

Member State:

Belgium

12 JULY 2019. - Royal Decree Implementing the Law of 7 April 2019 Establishing a Framework for the Security of Network and Information Systems of General Interest for Public Security, as well as the Law of 1 July 2011 on the Security and Protection of Critical Infrastructures

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

12 JULY 2019. - Royal Decree Implementing the Law of 7 April 2019 Establishing a Framework for the Security of Network and Information Systems of General Interest for Public Security, as well as the Law of 1 July 2011 on the Security and Protection of Critical Infrastructures

CHAPTER 1. Purpose

Article 1

The purpose of this Order is to transpose European Directive (EU) 2016/1148 of 6 July 2016 on measures to ensure a common high level of security of networks and information systems in the Union (the "NIS Directive").

CHAPTER 2. Definitions

Art. 2.

For the purposes of this Royal Decree, the following definitions shall apply
(1) "Act" means the Act of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security;
2° "CCB": the Centre for Cybersecurity Belgium created by the Royal Decree of 10 October 2014;
3° "DGCC": the Directorate General Crisis Centre of the Federal Public Service of the Interior, created by the Royal Decree of 18 April 1988 establishing the Governmental Coordination and Crisis Centre;
4° "notification platform": the incident notification platform referred to in Article 31 of the Act.

CHAPTER 3. Competent authorities

Art. 3.

§ 1. The BAC is designated as the authority referred to in Article 7 § 1 and Article 10 § 1 of the Act.
The BAC is designated as the national CSIRT referred to in Article 7, § 2 of the Act.
§ 2. The DGCC is designated as the authority referred to in Article 7, § 4, of the Act.
§ 3. The sectoral authorities referred to in Article 7(3) of the Act are designated in Annex 1.
§ 4. The inspection services referred to in Article 7, § 5 of the Act are designated in Annex 2.

Art. 4.

§ 1. For critical infrastructures in the health sector, the sectoral authority referred to in Article 3, 3°, f) of the Act of 1 July 2011 on the security and protection of critical infrastructures is designated in Annex 1, point c).
§ 2. For critical infrastructure in the health sector, the inspection service referred to in Article 24(2) of the Act of 1 July 2011 on security and protection of critical infrastructure is designated in

Annex 2(a).

CHAPTER 4. Notification and processing of incidents

Section 1. Scope and notification platform

Art. 5.

This chapter shall apply to incident notifications referred to in Articles 24, 26, § 1, 27, 31 and 35 of the Act of 7 April 2019.

Art. 6.

A secure notification platform is created to facilitate:
1° the sending by operator of essential services and digital service providers to the national CSIRT, the sectoral authority or its sectoral CSIRT, and the DGCC, of notifications of security incidents made under the Act of 7 April 2019;
2° the possibility for operators of essential services and digital service providers to send notification of personal data breaches to a personal data control authority, as provided for by Article 31, § 1, paragraph 2, and by Article 36, § 2, of the Act.

Art. 7.

The platform referred to in Article 6 shall be accessible via the Internet for operator of essential services and digital service providers by means of a secure connection and the use of an identification key unique to each operator of essential services or digital service provider.

Section 2. Notifications

Art. 8.

§ 1. The notification is made via the notification platform and using the incident notification form determined by the national CSIRT.
The notification shall contain all available information to determine the nature, causes, effects and consequences of the incident.
§ 2. Where the operator of essential services or digital service provider is unable to provide all the information in the form using the elements in its possession, it shall complete the initial notification via the notification platform as soon as the missing information is available.
§ 3. It does the same when new information is known or when important developments occur.
§ 4. At the request of the national CSIRT, the DGGC, the sector authority or its sector CSIRT, the essential services operator or the digital service provider notifies via the notification platform an update of the notification form tracing the management of the incident from its discovery to its closure and including all the information contained in the notification form.

Art. 9.

In the event of unavailability of the notification platform referred to in Article 6, the national CSIRT shall inform operator of essential services and digital service providers of the operational modalities of notification to be used.

Section 3. Treatment of the incident

Art. 10.

§ 1. The national CSIRT, the sectoral authority or its sectoral CSIRT, or the DGCC may ask the operator of essential services or digital service provider for additional information on the notifications it has made.
§ 2. Where circumstances permit, the national CSIRT shall provide the operator of essential services or digital service provider that initiated the notification with all information relevant to the follow-up of the notification and, where appropriate, all information that could contribute to the effective management of the incident.
§ 3. Without prejudice to the rules applicable to crisis management in the event of cyber incidents referred to in Article 3, 5°, of the Royal Decree of 10 October 2014 establishing the Centre for Cybersecurity Belgium, the national CSIRT ensures the coordination of the processing of notifications at national and international level.

Section 4. Memorandum of Understanding

Art. 11.

The national CSIRT, the sectoral authorities and the DGCC conclude a memorandum of understanding to establish the operational modalities:
1° management of the notification platform;
2° the processing of the notifications referred to in Article 8, § 3;
3° requests for additional information to the operator of essential services or digital service provider referred to in Article 6, § 4.

CHAPTER 5. Voluntary notifications

Art. 12.

§ 1. The voluntary notifications referred to in article 30 of the Act shall be addressed directly to the national CSIRT.
§ 2. The operational details of this notification are determined by the national CSIRT and published on its website.
§ 3. The national CSIRT forwards the information on these notifications to the DGCC and to the sectoral authorities or sectoral CSIRTs potentially concerned.

CHAPTER 6. Derogations

Art. 13.

Chapters IV and V are derogated from for notifications of personal data breaches, which follow the legal rules or imposed by the personal data supervisory authority referred to in Article 6, 4°, of the Law of 7 April 2019.

CHAPTER 7. Conformity assessment bodies

Art. 14.

Conformity assessment bodies wishing to be accredited for the external audit and certification of operators of essential services, as referred to in articles 22, § 2, and 38, § 2, of the Act, or for the external audit of digital service providers, shall apply to the national accreditation authority or to an institution that is a co-signatory to the recognition agreements of the European Cooperation for Accreditation.
The conditions that the conformity assessment body must meet in order to be accredited for this purpose are as follows:
1. meet, at all times, the accreditation criteria laid down in ISO/IEC 17021 or ISO/IEC 17065, which specify (a) the generic and specified requirements for bodies providing audit and

certification of management systems and; (b) the requirements to ensure that certification bodies operate certification schemes competently, consistently and impartially;

2. comply with the operating procedures of the accreditation system applicable to accredited bodies.

CHAPTER 8. Final provisions

Art. 15.

This decree shall enter into force on the day of its publication in the Moniteur belge.

Art. 16.

The Prime Minister and the Minister for Security and the Interior are responsible, each in his or her own area of responsibility, for the execution of this decree.

ANNEXES

Art. N1. Appendix 1.

The sectoral authorities designated by Us:

a) for the energy sector: the Federal Minister responsible for Energy or, by delegation of the latter, a senior member of the staff of his administration (if necessary, the Minister may designate a different delegate for each sub-sector)

b) for the transport sector:

- With regard to the transport sector, with the exception of transport by waterways accessible to sea-going vessels: the Federal Minister responsible for Transport, or by delegation of the latter, a senior member of the staff of his administration (if necessary, the Minister may designate a different delegate for each sub-sector);
- As regards transport by waterways accessible to maritime vessels: the Federal Minister responsible for Maritime Mobility, or by delegation of the latter, a senior member of the staff of his administration (if necessary, the Minister may designate a different delegate for each sub-sector);

c) for the health sector: the Federal Minister responsible for Public Health or, by delegation of the latter, a senior member of the staff of his or her administration (if necessary, the Minister may designate a different delegate for each sub-sector);

d) for the digital service provider sector: the Federal Minister for Economic Affairs or, by delegation of the latter, a senior member of the staff of his administration (if necessary, the Minister may designate a different delegate for each sub-sector).

Art. N2. Annex 2.

The inspection services designated by Us:

a) for the health sector: the federal public service Public Health;

b) for the energy sector, with the exception of those parts of a nuclear installation intended for the industrial production of electricity which are used for the transmission of electricity: the Federal Public Service Economy;

c) for the digital service provider sector: the Federal Public Service Economy.