EnCaViBS

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

Member State:

France

Act No. 2018-133 of 26 February 2018 on various provisions for adapting to European Union law in the field of 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: France

Act No. 2018-133 of 26 February 2018 on various provisions for adapting to European Union law in the field of security

JORF n°0048 of 27 February 2018

The National Assembly and the Senate have adopted the bill,

The President of the Republic promulgates the following law:

Title I: PROVISIONS TRANSPOSING DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 6 JULY 2016 CONCERNING MEASURES FOR A HIGH COMMON LEVEL OF SECURITY OF NETWORK AND INFORMATION SYSTEMS ACROSS THE UNION (Articles 1 to 15)

Chapter I: Common provisions (Articles 1 to 4)

Article 1

For the purposes of this Title, network and information system shall mean:

1. Any electronic communications network as defined in 2° of Article L. 32 of the Post and Electronic Communications Code;

2. Any device or set of interconnected or related devices, one or more of which, while executing a program, performs automated processing of digital data;

3. The digital data stored, processed, retrieved or transmitted by the elements mentioned in 1° and 2° of this article for their operation, use, protection and maintenance.

The security of networks and information systems means their capacity 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.

Article 2

The provisions of this Title are not applicable to the operators mentioned in 15° of Article L. 32 of the French Post and Electronic Communications Code for their activities related to the operation of electronic communications networks or the provision of electronic communications services, or to trust service providers subject to the requirements set out in Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Nor shall they be applicable to operators of critical services or digital service providers for the networks and information systems mentioned in the first paragraph of Articles 5 and 12 of this Act, which are subject, pursuant to a legal act of the European Union, to sectoral security and incident reporting requirements having an effect at least equivalent to the obligations resulting from the application of this Title.

Article 3

I. - Service providers authorised to carry out checks under this title are subject to the same rules of confidentiality and professional discretion as public officials and Government services with regard to the information they gather from the operators mentioned in Article 5 and the digital service providers mentioned in Article 11.

II. - When informing the public or EU Member States of incidents under the conditions provided for in Articles 7 and 13, the competent administrative authority shall consider the economic interests of these operators and digital service providers and shall ensure that it does not disclose information that could undermine their security and commercial and industrial secrecy.

Article 4

The procedures for the application of this title shall be determined by decree in the Council of State. This decree shall determine the list of services critical for the functioning of society or the economy mentioned in Article 5 and, for each of the areas of security mentioned in Article 12, the nature of the measures that digital service providers are required to implement.

Chapter II: Provisions on the security of networks and information systems of operators of critical services (Articles 5 to 9)

Article 5

Public or private operators providing services critical for the functioning of society or the economy and whose continuity could be seriously affected by incidents affecting the networks and information systems necessary for the provision of said services shall be subject to the provisions of this Chapter. These operators are designated by the Prime Minister. The list of these operators shall be updated at regular intervals and at least every two years. The provisions of this chapter shall not apply to the operators mentioned in Articles L. 1332-1 and L. 1332-2 of the Defence Code, for the information systems mentioned in the first paragraph of Article L. 1332-6-1 of the same code.

Article 6

The Prime Minister shall lay down the security rules necessary for the protection of the networks and information systems mentioned in the first paragraph of Article 5. The purpose of these rules is to guarantee a level of security appropriate to the existing risk, taking current knowledge into account. They shall define appropriate measures to prevent or limit the impact of incidents that compromise the security of networks and information systems used for the provision of critical services in order to ensure the continuity of those critical services. The operators mentioned in Article 5 shall apply these rules at their own expense. The rules provided for in the first paragraph of this Article shall be defined in each of the following areas:

1. The governance of network and information system security

2. The protection of networks and information systems;

3. The defence of networks and information systems;

4. The resilience of activities.

The rules provided for in the same subparagraph may, inter alia, require operators to use hardware or software devices or computer services whose security has been certified.

Article 7

I. - The operators mentioned in Article 5 shall report, immediately after becoming aware of it, to the national information systems security authority mentioned in Article L. 2321-1 of the Defence Code, any incidents affecting networks and information systems necessary for the provision of critical services, where these incidents have or are likely to have, considering the number of users and the geographical area affected and the duration of the incident, a significant impact on the continuity of these services.

II. - After consulting the relevant operator, the administrative authority may inform the public of an incident mentioned in I of this article, where such information is necessary to prevent or deal with an incident. Where an incident has a significant impact on the continuity of critical services provided by the operator in other EU Member States, the administrative authority shall inform the competent authorities or bodies in those States.

Article 8

The Prime Minister may subject the operators referred to in Article 5 to checks intended to verify compliance with the obligations set out in this chapter and the level of security of the networks and information systems necessary for the provision of critical services.

Checks shall be carried out, on the basis of documents and in situ, by the national authority for information systems security mentioned in Article L. 2321-1 of the Defence Code or by service providers qualified by the Prime Minister. The cost of the checks shall be borne by the operators.

Operators shall be required to provide the authority or service provider responsible for the supervision provided for in the first paragraph of this article with the information and elements necessary to carry out the supervision, including documents relating to their security policy and, as applicable, the results of security audits, and to give them access to the networks and information systems under supervision in order to carry out analyses and technical information surveys.

In the event of a failure to meet an obligation established during a check, the authority referred to in the second paragraph may give formal notice to the management of the relevant operator to meet the obligations incumbent on the operator under this Chapter within a deadline which it shall determine. The deadline is determined in consideration of the operating conditions of the operator and the measures to be implemented.

Article 9

A fine of €100,000 shall be imposed on the managers of the operators mentioned in Article 5 for failing to comply with the security rules mentioned in Article 6 at the end of the period set by the formal notice sent to them pursuant to Article 8.

A fine of €75,000 shall be imposed on the same persons for breaching the obligation to report an incident as provided for in Article 7(I).

A fine of €125,000 shall be imposed on the same persons for obstructing the supervisory operations mentioned in Article 8.

Chapter III: Provisions on the security of networks and information systems of digital service providers (Articles 10 to 15)

Article 10

For the purposes of this chapter, the following definitions apply

1. A digital service is any service normally provided for consideration, remotely, by electronic means and at the individual request of a recipient of services;

2. A digital service provider is any legal entity that provides any of the following services:

a) Online marketplace, that is to say a digital service which enables consumers or professionals, as per the last paragraph of the introductory article of the Consumer Code, to conclude contracts of sale or service online with professionals either on the website of the online marketplace or on the website of a professional who uses the IT services provided by the online marketplace;

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

c) Cloud computing service, or a digital service that provides access to a scalable and variable set of computing resources that can be shared.

Article 11

I. - Any digital service provider pursuant to Article 10, established outside the European Union, which offers its services on domestic soil and which has not designated a representative in another Member State of the European Union shall designate a representative established on domestic soil vis a vis the national information systems security authority provided for in Article L. 2321-1 of the Defence Code for the purposes of this chapter. This designation shall not preclude any action which may be brought under Article 15 against the directors of the supplier concerned.

II. - Digital service providers offering their services in the European Union shall be subject to the provisions of this Chapter:

1. When their registered office or main place of business is established on domestic soil;

2. Or who have, in application of I, designated a representative on domestic soil.

III. - The provisions of this chapter are not applicable to companies employing less than fifty employees and whose annual turnover is below 10 million euros.

Article 12

The digital service providers referred to in Article 11 shall ensure, considering the state of the art, a level of security of the networks and information systems necessary for the provision of their services in the European Union appropriate to the risks involved. To this end, they are required to identify the risks to the security of those networks and information systems and to take the necessary and proportionate technical and organisational measures to manage those risks, to prevent any incidents that could harm those networks and information systems and to minimise their impact, such as to ensure the continuity of their services. These measures apply in each of the following areas:

1 The security of systems and installations;

2. Incident management;

3. Business continuity management;

4. Monitoring, audit and supervision;

5. Compliance with international standards.

Article 13

I. The digital service providers mentioned in Article 11 shall report, immediately after becoming aware of it, to the national information systems security authority mentioned in Article L. 2321-1 of the Defence Code, any incidents affecting the networks and information systems necessary for the provision of their services in the European Union, where the information available to them indicates that such incidents have a significant impact on the provision of these services, considering the number of users affected by the incident, its duration, its geographical scope, the seriousness of the disruption to the functioning of the service and the extent of its impact on the functioning of society or the economy.

II. After consulting the relevant digital service provider, the administrative authority may inform the public of an incident referred to in I or require the provider to do so where such information is necessary to prevent or deal with an incident or is justified by a reason of public interest. Where an incident has a significant impact on services provided in other EU Member States, the administrative authority shall inform the competent authorities or bodies in those States, which may make the incident public.

Article 14

When the Prime Minister is informed that a digital service provider referred to in Article 11 has breached one of the obligations set out in Articles 12 or 13, he may subject it to checks designed to verify compliance with the obligations set out in this chapter and the level of security of the networks and information systems required to render its services. If necessary, it shall inform and cooperate

with the competent authorities of the other EU Member States in which networks and information systems of that provider are located.

Checks shall be carried out, on the basis of documents and in situ, by the national authority for information systems security mentioned in Article L. 2321-1 of the Defence Code or by service providers qualified by the Prime Minister. The cost of the checks is borne by the digital service providers. Digital service providers shall be required to provide the authority or service provider responsible for the supervision provided for in the first paragraph of this Article with the information necessary to assess the security of their networks and information systems, including documents relating to their security policies, and, as applicable, to allow access to the networks and information systems subject to supervision in order to carry out analyses and technical information surveys.

In the event of a failure to meet an obligation established during a check, the authority referred to in the second paragraph may give formal notice to the management of the relevant provider to meet the obligations incumbent on it under this Chapter within a deadline which it shall determine. The deadline is determined in consideration of the operating conditions of the provider and the measures to be implemented.

Article 15

A fine of €75,000 shall be imposed on the managers of the digital service providers mentioned in Article 11 for failing to comply with the security rules mentioned in Article 12 at the end of the period set by the formal notice sent to them pursuant to Article 14.

A fine of €50,000 shall be imposed on the same persons for breaching the obligation to report an incident or inform the public as provided for in Article 13(I).

A fine of €100,000 shall be imposed on the same persons for obstructing the supervisory operations mentioned in Article 14.

Title II: PROVISIONS RELATING TO CONTROL OF THE ACQUISITION AND HOLDING OF WEAPONS (Articles 16 to 22)

…

Title III: PROVISIONS RELATING TO THE REGULATED PUBLIC SERVICE OF BROADCASTING BY SATELLITE (Article 23)

…

Title IV: PROVISIONS APPLICABLE TO OVERSEAS (Article 24)

…

Title V: TRANSITIONAL PROVISIONS (Article 25)

…

Done in Paris, 26 February 2018.