EnCaViBS

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

Member State:

Sweden

Law (2018:1174) on information security for essential and digital services

(consolidated version including SFS 2018:1176)

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: Sweden

Law (2018:1174) on information security for essential and digital services

(consolidated version including SFS 2018:1176)

Purpose of the law

1§. The purpose of this law is to achieve a high level of security in networks and information systems for

1. essential services within the following sectors
   - energy,
   - transport,
   - banking activity,
   - financial market infrastructure,
   - health and medical care,
   - supply and distribution of drinking water,
   - digital infrastructure, and
2. digital services.

Terms used in the law

2§. For the purposes of the law,

1. network and information system means:
   a) an electronic communications network as defined in Chapter 1, Section 7 of the law (2003:389) on electronic communication,
   b) a device or a group of devices that are linked together or belong with each other, one or more of which use a program to carry out the automatic processing of digital data, or
   c) digital data that is stored, processed, retrieved or transferred by the means referred to in a) and b), to enable it to be operated, used, protected and maintained,
2. security of a network and information system means:
   the ability of the network and information system to resist, to some degree of reliability, actions that undermine the accessibility, authenticity, accuracy or confidentiality of stored, transferred or processed data or of the related services provided through or available via these networks and information systems,
3. essential service means:
   a service that is important for maintaining critical societal or economic activity,
4. digital service means:
   a service that is defined in Article 1.1 b of European Parliament and Council Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on information society services, and which constitutes an internet-based marketplace, internet-based search engine or cloud service,
5. internet-based market place means:
   a service that makes it possible for consumers or operators, as defined in Article 4.1 a and 4.1 b of European Parliament and Council Directive 2013/11/EU of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) 2006/2004 and Directive 2009/22/EC (Alternative Dispute Resolution Directive) to enter into internet-based purchase agreements or service agreements with traders, either on the website of the internet-based market place or on the website belonging to an operator and where data services provided by an internet-based market place are used,
6. internet-based search engine means:

a service that makes it possible for users to carry out searches on practically all websites, or websites in a specific language, by making an enquiry on any subject in the form of a key word, a phrase or some other input, and which returns links containing information on the required content,

7. cloud service means:
   a service that makes it possible to access a scalable and elastic pool of sharable data resources,
8. The NIS Directive means:
   European Parliament and Council Directive (EU) 2016/1148 of 6 July 2016 concerning measures to achieve a high common level of security of networks and information systems across the Union,
9. representative means:
   a natural or legal person explicitly appointed to act for a operator, that authorities are able to refer to instead of the operator in matters concerning the operator's obligations under the NIS Directive,
10. incident means:
    an event that has an actual negative effect on the security of networks and information systems, and
11. risk means:
    a reasonably identifiable circumstance or event that has a potential negative effect on the security of networks and information systems.

Area of application of the law

3§. The law applies to

1. operators of the kind referred to in Annex 2 to the NIS Directive and who provide a essential service, on condition that the operator is established in Sweden, that the provision of the services is dependent on networks and information systems, and that an incident would lead to a significant disruption to the service provision (providers of essential services), and
2. legal entities that provide a digital service and whose principal establishment is in Sweden, or that have appointed a representative who is established here (providers of digital services).

Section 10 contains a provision that applies to other operators.

4§. The government, or the person designated by the government, may issue regulations on which services are essential, and what is meant by significant disruption, as mentioned in Section 3, Paragraph 1 (1).

Exceptions to the area of application of the law

Providers of electronic communication services

5§. The law does not apply to companies that provide public communication networks or publicly available electronic communication services and are therefore bound by the requirements of Chapter 5, Section 6 b) and c) of the law (2003:389) on electronic communication.

Providers of trusted services

6§. The law does not apply to providers of trusted services covered by the requirements of Article

19 of European Parliament and Council Regulation (EU) 910/2014 of 23 July 2014 on electronic identification and trusted services for electronic transactions in the internal market, and repealing Directive 1999/93/EC.

Providers of digital services that are micro or small enterprises
7§. The law does not apply to providers of digital services that are micro-companies or small companies as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

Security-sensitive Activity
8§. The law does not apply to activity that is subject to the Security Protection Law (2018:585).
Law (2018:1176).

Operators bound by requirements for information security in other statutes
9§. If a law or other statute contains provisions with requirements for security measures and incident reporting, these provisions shall apply if the effect of the requirements is at least equal to the effect of the obligations under this law, considering the scope of the provisions and what supervision and sanctions are necessitated by the requirements of the provisions.

Appointment of representatives
10§. A legal entity that provides digital services in Sweden but whose principal establishment is not within the European Union, and which has not appointed a representative who is established in a member state where the services are provided, shall appoint such representative, unless an exception to the law's area of application under Sections 5-9 applies.

Security measures

Obligations of operators of essential services
11§. Operators of essential services shall implement systematic and risk-based information security measures in relation to the networks and information systems they use to provide essential services.

12§. Operators of essential services shall carry out a risk assessment on which the choice of security measures referred to in Sections 13 and 14 shall be based. The assessment shall include an action plan. The assessment shall be documented and updated annually.

13§. Operators of essential services shall implement appropriate and proportional technical and organisational measures to manage risks that threaten the security of the networks and information systems they use to provide essential services. These measures must ensure a level of security of the networks and information systems that is appropriate to the risk.

14§. Operators of essential services shall implement appropriate measures to prevent and minimise the effect of incidents on the networks and information systems they use to provide essential services. The measures must aim to ensure continuity of the services.

Obligations of digital service providers
15§. Digital service providers shall implement the technical and organisational measures they consider appropriate and proportionate to manage risks that threaten the security of the networks and information systems they use when providing digital services within the European Union. These

measures must ensure a level of security of the networks and information systems that is appropriate to the risk.

16§. Digital service providers shall implement measures to prevent and minimise the effect of incidents on the networks and information systems they use. The obligation only applies in respect of the effects such incidents have on the digital services provided by the provider within the European Union. The measures must aim to ensure continuity of the services.

Authorisation
17§. The government, or the authority appointed by the government, may issue regulations on the security measures referred to in Sections 11-16.

Incident reporting

Reporting obligation of operators of essential services
18§. Operators of essential services shall, without undue delay, report incidents that have a significant effect on the continuity of the essential service they provide. The reporting shall be made to the authority appointed by the government.

Reporting obligation of digital service providers
19§. Digital service providers shall, without undue delay, report incidents that have a considerable effect on the provision of the digital service they provide within the European Union. The reporting shall be made to the authority appointed by the government.

Authorisation
20§. The government, or the authority appointed by the government, may issue regulations on the incident reporting referred to in Sections 18 and 19.

Supervision

Task of the supervisory authority
21§. The authority appointed by the government is the supervisory authority. The supervisory authority shall undertake supervision to ensure that this law and the regulations issued in connection with it are complied with.

22§. Supervisory measures may only be taken in respect of providers of digital services when the supervisory authority has a legitimate reason to assume that a provider does not meet the requirements of Section 15, 16 or 19.

Registration obligation of operators of essential services
23§. Operators of essential services shall register with the supervisory authority without delay. It must be clear from the registration whether the operator provides an essential service in two or more member states of the European Union.

The supervisory authority’s powers to investigate
24§. A person under supervision shall provide the supervisory authority with the information needed for the supervision on request.

25§. The supervisory authority has the right to access the areas, premises and other spaces, but not dwellings, which are used in the activity covered by the law, in the extent needed for the supervision.

26§. The supervisory authority may order a person under supervision to provide the information and grant the access mentioned in Sections 24 and 25.

Such an order may be combined with a fine.

27§. The supervisory authority may request the assistance of the Swedish Enforcement Authority to implement the measures referred to in Sections 24 and 25. The provisions of the Enforcement Code on the execution of obligations that do not relate to a payment obligation, eviction or removal, apply to this assistance.

Interventions and sanctions

Remedial injunctions

28§. The supervisory authority may issue injunctions that are needed for operators to meet the requirements for the appearance of representatives, security measures and incident reporting referred to in Sections 10, 12-16, 18 and 19 and in regulations issued in connection with these paragraphs.

Such an order may be combined with a fine.

Penalty fee

29§. The supervisory authority shall charge a penalty fee to a person who fails to

1. register with the supervisory authority in accordance with Section 23 or regulations issued in connection with this paragraph,
2. implement the security measures in accordance with any of Sections 12-16 or regulations issued in connection with those paragraphs, or
3. report incidents in accordance with Section 18 or 19 or regulations issued in connection with those paragraphs.

30§. A penalty fee shall be set at a minimum of SEK 5,000 and a maximum of SEK 10,000,000.

31§. The determination of the size of the fee shall take particular account of the damage or risk of damage caused as a consequence of the contravention, if the operator has previously committed a contravention, and the costs the operator has avoided as a consequence of the contravention.

32§. A penalty fee may be waived in whole or in part if the contravention is minor or unintentional, or if it would otherwise be unreasonable to charge the fee considering the circumstances.

33§. A decision to charge a penalty fee may not be made if the contravention is subject to a fine and the contravention forms the basis for an application to impose the fine.

34§. The decision to charge a penalty fee may only be made if the person who is charged the fee has had the opportunity to make a statement within two years of the contravention.

A decision to charge a penalty fee must be served.

35§. A penalty fee must be paid to the supervisory authority within 30 days of the date the decision to charge the fee becomes legally binding, or the period specified in the decision if this is longer.
If the penalty fee is not paid within the time stated in the first paragraph, the authority shall refer the unpaid fee for debt collection. Provisions on debt collection are contained in the law (1993:891) on the recovery of state receivables, etc. Enforcement shall comply with the Enforcement Code.

Penalty fees accrue to the state.

36§. A penalty fee lapses if the decision to charge the fee is not enforced within five years of when the decision becomes legally binding.

Regulations on enforcement
37§. The government, or the authority appointed by the government, may issue regulations under Chapter 8, Section 7 of the Instrument of Government, on the enforcement of this law.

Ruling that a decision should have immediate effect
38§. The supervisory authority may rule that a decision on an order under this law shall have immediate effect.

Appeals
39§. A decision made by the supervisory authority in accordance with this law may be appealed to an ordinary administrative court. When such a decision is appealed, the supervisory authority is the counterparty in court. Leave to appeal is required is the decision is appealed to the administrative court of appeal.