EnCaViBS

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

Member State:

Sweden

Regulation (2018:1175) on information security for essential and digital services

(consolidated version including SFS 2020:1142)

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

Regulation (2018:1175) on information security for essential and digital services

(consolidated version including SFS 2020:1142)

Introductory provision

1§. This regulation supplements the law (2018:1174) on information security for essential and digital services, and the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of European Parliament and Council Directive (EU) 2016/1148 concerning measures for a high common level of security of networks and information systems across the Union, as regards more detailed specification of the aspects that providers of digital services must take into account when managing risks that threaten the security of their networks and information systems, and the parameters for determining whether an incident has a considerable effect, referred to here as the Commission Implementing Regulation, on digital service providers.

Terms used in this regulation

2§. Terms used in this regulation have the same meaning as those used in the law (2018:1174) on information security for essential and digital services.

For the purposes of this regulation,

1. standard means:
   a standard that is defined in Article 2.1 of European Parliament and Council Regulation (EU) 1025/2012 of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and European Parliament and Council Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC, and repealing Council Decision 87/95/EEC and European Parliament and Council Decision 1673/2006/EC,
2. specification means:
   a technical specification as defined in Article 2.4 European Parliament and Council Regulation (EU) 1025/2012, and
3. CSIRT unit means:
   Sweden’s unit for the management of incidents reported in accordance with the European Parliament and Council Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of networks and information systems across the Union (the NIS Directive).

Services that are essential

3§. The Swedish Civil Contingencies Agency may issue regulations, after giving the supervisory authorities and the National Board of Health and Welfare the opportunity to comment, on what services are essential services according to the law (2018:1174) on information security for essential and digital services. The regulations must be updated at least every other year.

Significant disruption to continuity of an essential service

4§. In the assessment of what is considered a significant disruption as referred to in Section 3, Paragraph 1 (1) of the law (2018:1174) on information security for essential and digital services, the

following cross-sector factors must be considered:

1. the number of users who depend on the service provided by the operator concerned,
2. the level of dependency of other sectors covered by the NIS Directive on the service provided by the operator,
3. what effect incidents could have on financial and societal activity or public security, expressed in terms of degree and duration,
4. the operator's share of the market,
5. how large a geographical area could be affected by an incident, and
6. the operator's significance for maintaining an adequate service level, taking alternative ways of providing the service into account.

Sector-specific factors should also be considered where appropriate.

The Swedish Civil Contingencies Agency may issue regulations, after giving the supervisory authorities and the National Board of Health and Welfare the opportunity to comment, on what is meant by significant disruption.

Security measures

Standards and specifications

5§. When formulating security measures, operators of essential services and providers of digital services shall consider European and internationally accepted standards and specifications.

Technical and organisational measures

6§. In the assessment of whether the security measures referred to in Section 15 of the law (2018:1174) on information security for essential and digital services ensures a level of security of networks and information systems that is appropriate to the risk, the following shall be taken into consideration:

1. the security of the system and facilities,
2. incident management,
3. management of operational continuity,
4. monitoring, revision and testing, and
5. compliance with international standards.

Article 2 of the Commission Implementing Regulation concerning digital service providers contains provisions that further describe what is meant by points 1-5 in the first paragraph.

Further regulations on security measures

7§. The Swedish Civil Contingencies Agency may issue regulations, after giving the supervisory authorities and the National Board of Health and Welfare the opportunity to comment, on systematic and risk-based information security work according to Section 11 of the law (2018:1174) on information security for essential and digital services.

8§. The Swedish Energy Agency, Transport Agency, Financial Supervisory Authority, National Food Agency, and Post and Telecom Authority may issue regulations on security measures in accordance with Sections 12-14 of the law (2018:1174) on information security for essential and digital services for their respective areas of supervision.

The National Board of Health and Welfare may issue such regulations for the Health and Social Care Inspectorate's area of supervision. Before the regulations are issued, the Civil Contingencies Agency is given the opportunity to comment.
The Civil Contingencies Agency shall give the supervisory authorities and the National Board of Health and Welfare advice and support when drafting the regulations.

Incident reporting

Significant impact on continuity of an essential service

9§. In the assessment of whether an incident has a significant imapct on the continuity of an essential service in accordance with Section 18 of the law (2018:1174) on information security for essential and digital services, the following shall be taken into consideration:

1. the number of users affected by the disruption to the essential service,
2. how long the incident lasts, and
3. how large a geographical area is affected by the incident.

The Swedish Civil Contingencies Agency may issue regulations, after giving the supervisory authorities and the National Board of Health and Welfare the opportunity to comment, on what is meant by significant impact.

Substantial impact on the provision of a digital service

10§. In the assessment of whether an incident has a substantial impact on the provision of a digital service in accordance with Section 19 of the law (2018:1174) on information security for essential and digital services, the following shall be taken into consideration:

1. the number of users affected by the incident, especially users who depend on the service to be able to provide their own services,
2. how long the incident lasts,
3. how large a geographical area is affected by the incident,
4. to what extent the incident disrupts the service's function, and
5. to what extent the incident affects the economic and societal activity.

Articles 3 and 4 of the Commission Implementing Regulation concerning digital service providers contains further provisions on what is considered to a substantial impact.

Digital service providers are only obliged to report incidents if they have access to the information that is needed to assess whether an incident has a substantial impact.

To which authority the incident reporting must be made

11§. Incident reporting under the law (2018:1174) on information security for essential and digital services shall be made to the CSIRT unit.

CSIRT unit

12§. The Swedish Civil Contingencies Agency is a CSIRT unit.

The CSIRT unit shall

1. receive incident reports that are provided under the law (2018:1174) on information security for essential and digital services in accordance with regulations issued in connection with the law,

2. make the information in incident reports available to the supervisory authorities and the National Board of Health and Welfare without delay, and
3. promptly urge operators to report incidents that are assumed to be based on a criminal act to the Swedish Police Authority.

The CSIRT unit shall also meet the requirements and complete the tasks specified in Annex 1 to the NIS Directive, and in some cases inform reporting suppliers, other member states and the public of incidents, in accordance with Articles 14.5, 14.6, 16.6 and 16.7 of the NIS Directive.

Content of an incident report

13§. An incident report shall contain information that enables the CSIRT unit to determine the extent of the incident's cross-border effects.

The Swedish Civil Contingencies Agency may issue regulations, after giving the supervisory authorities and the National Board of Health and Welfare the opportunity to comment, on what information an incident report should contain.

Enforcement regulations on incident reporting

14§. The Swedish Civil Contingencies Agency may issue further regulations on the time scale for incident reporting and the specific forms of reporting in accordance with Sections 18 and 19 of the law (2018:1174) on information security for essential and digital services.

Voluntary reporting of incidents

15§. The Swedish Civil Contingencies Agency may issue regulations, after giving the supervisory authorities and the National Board of Health and Welfare the opportunity to comment, on the voluntary reporting of incidents in accordance with Article 20 of the NIS Directive for operatpors that are not providers of essential or digital services.

Registration obligation of providers of essential services

16§. The Swedish Civil Contingencies Agency may issue further regulations, after giving the supervisory authorities the opportunity to comment, on the obligation to register contained in Section 23 of the law (2018:1174) on information security for essential and digital services. The regulations may specify when registration is required, what information a registration should contain, and the specific ways in which the obligation to register can be met.

Supervision

Supervisory authorities

17§. The following authorities are supervisory authorities in the sectors shown for operators of essential services, according to the law (2018:1174) on information security for essential and digital services:

Supervisory authority	Sector
The Swedish Energy Agency	Energy
The Swedish Transport Agency	Transport

The Financial Supervisory Authority	Banking activity
The Financial Supervisory Authority	Financial market infrastructure
The Health and Social Care Inspectorate	Health and medical care
The National Food Agency	Supply and distribution of drinking water
The Post and Telecom Authority	Digital infrastructure

18§. The Swedish Post and Telecom Authority is the supervisory authority for providers of digital services, according to the law (2018:1174) on information security for essential and digital services.

The supervisory authority's tasks

19§. */Ceases to apply U:01-01-2021/* The supervisory authorities shall, for their respective areas of supervision,

1. provide the Swedish Civil Contingencies Agency with information on the content of registrations made in accordance with Section 23 of the law (2018:1174) on information security for essential and digital services,
2. by no later than 20 September every two years, starting from 2020, provide the Civil Contingencies Agency with the details of the essential service providers under the authority's supervision, broken down by sectors and sub-sectors, as specified in Annex 2 to the NIS Directive, as well as details of the providers' significance for these sectors,
3. give general guidance, within the scope of its supervision, on the application of the law (2018:1174) on information security for essential and digital services, and of regulations issued in connection with the law,
4. cooperate with the Swedish Data Inspection Authority on the management of incidents that are also personal data incidents,
5. provide support for Sweden's representative in the cooperation group established in accordance with Article 11 of the NIS Directive, and
6. cooperate with and assist supervisory authorities in other EU member states in respect of legal entities providing digital services whose principal establishment is in other member states, or who have appointed representatives in other member states.

19§. */Enters into force U:01-01-2021/* The supervisory authorities shall, for their respective areas of supervision,

1. provide the Swedish Civil Contingencies Agency with information on the content of registrations made in accordance with Section 23 of the law (2018:1174) on information security for essential and digital services,
2. by no later than 20 September every two years, starting from 2020, provide the Civil Contingencies Agency with the details of the essential service providers under the authority's supervision, broken down by sectors and sub-sectors, as specified in Annex 2 to the NIS Directive, as well as details of the providers' significance for these sectors,
3. give general guidance, within the scope of its supervision, on the application of the law (2018:1174) on information security for essential and digital services, and of regulations issued in connection with the law,
4. cooperate with the Swedish Authority for Privacy Protection on the management of incidents that are also personal data incidents,
5. provide support for Sweden's representative in the cooperation group established in accordance with Article 11 of the NIS Directive, and

6. cooperate with and assist supervisory authorities in other EU member states in respect of legal entities providing digital services whose principal establishment is in other member states, or who have appointed representatives in other member states. *Regulation (2020:1142).*

Request for information

20§. When a supervisory authority requests information under Section 24 of the law (2018:1174) on information security for essential and digital services, the authority shall state the purpose of the request and specify what information is required.

Partnership forum for effective and equal supervision

21§. The Swedish Civil Contingencies Agency shall manage a partnership forum that includes the supervisory authorities and the National Board of Health and Welfare. The purpose of the forum is to facilitate cooperation and ensure effective and equal supervision.

National point of contact

22§. The Swedish Civil Contingencies Agency is the single national point of contact, as required by the NIS Directive.

The national point of contact shall carry out the duties specified in Articles 8.4, 10.3 (2), and 14.5 (3) of the NIS Directive.

The national point of contact shall also fulfil Sweden’s obligation under Article 5.4 of the NIS Directive to consult with other member states and report the results of the consultation to the supervisory authority concerned.

Group for cooperation between the member states

23§. The Civil Contingencies Agency is Sweden’s representative in the cooperation group established in accordance with Article 11 of the NIS Directive.

Information to the Commission

24§. The Civil Contingencies Agency shall fulfil Sweden’s obligation under Article 5.7 of the NIS Directive to provide information on the implementation of the NIS Directive to the Commission.