EnCaViBS

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

Member State:

The Netherlands

Act dated 17 October 2018, concerning regulations for the implementation of directive (EU) 2016/1148 (Network and Information Systems Act)

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: Netherlands

Act dated 17 October 2018, concerning regulations for the implementation of directive (EU) 2016/1148 (Network and Information Systems Act)

Applicable as of 01-01-2019 up to and including 17-06-2020

Act dated 17 October 2018, concerning regulations for the implementation of directive (EU) 2016/1148 (Network and Information Systems Act)

We, Willem-Alexander, by the grace of God, King of The Netherlands, Prince of Oranje-Nassau, etc. etc. etc.

To all who see or read this, greetings! be it known:

We also took into consideration that within the scope of directive (EU) 2016/1148, it is necessary for setting down the statutory provisions necessary for promoting the security of network and information systems;

Thus, it is that We, having heard the advising department of the Council of State, and in general consultation with the parliament of the Netherlands, have approved and understood, and hereby We immediately agree and understand the following:

Chapter 1. Definitions

Article 1. (definitions)
For the purposes of this Act and the provisions based thereon:

- *supplier:* a government organisation or a private law legal entity which exploits, managers or makes a service available;
- *supplier of an essential service: a* supplier of an essential service as referred to in article 4 of the NIS directive, designated in conformity with article 5, paragraph one, under a;
- *the security of network and information systems, digital services, incidents, network and information systems, standards, or the risk of damage respectively:* that which is understood under article 4 of the NIS directive;
- *competent authority:* the competent authority referred to in article 4;
- *central point of contact:* the central point of contact as referred to in article 8, paragraph three of the NIS directive;
- *CSIRT:* Computer security incident response team as referred to in article 9 of the NIS directive;
- *CSIRT for digital services:* CSIRT, designated on the basis of article 4, paragraph two, under b;
- *digital service provider:* legal entity offering a digital service and which, in conformity with article 18, paragraphs one and two, of the NIS directive is under Dutch jurisdiction with the exception of small and microenterprises as referred to in article 16, paragraph eleven, of the NIS directive;
- *NIS directive:* 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 (PbEU 2016, L 194);
- *Our Minister:* Our Minister of Justice and Security;
- *vital provider:*

a. a supplier of an essential service;
b. the supplier of another service whose continuity is of vital importance for Dutch society.

Chapter 2. Our Minister's duties

Article 2. (central point of contact; CSIRT for essential services; authority for voluntary reports)
Our Minister is:

a. the central point of contact;
b. for suppliers of an essential service: the CSIRT;
c. the authority for the treatment of voluntary reports as referred to in article 16.

Article 3. (Our Minister's duties)

1 Our Minister has, for the prevention of the loss of availability or the loss of integrity of the network and information systems belonging to vital providers, and to other providers which are part of the national government, and for the further reinforcement of the digital resilience of Dutch society and for the execution of NIS directive, the following tasks:

a. the tasks of the central point of contact;
b. for suppliers of essential services: the CSIRT tasks listed in annex I, under 2, of the NIS directive;
c. offering support to the providers referred to in the preamble when implementing measures to guarantee or restore the continuity of their services;
d. informing and advising these providers and other in and outside of the Netherlands about any threats and incidents which relate to the network and information systems referred to in the preamble;
e. the execution of analyses and technical research for the benefit of the tasks listed under b, c and d, in response to the threats or incidents, or evidence thereof as referred to under d, but which do not relate to the investigation of individuals or organisations responsible for these threats or incidents, or which contribute to or have contributed to them in any way.

2 Furthermore, Our Minister has, for the prevention of adverse societal consequences in and outside of the Netherlands, been tasked with: issuing data, gathered within the context of paragraph one, under e, about threats and incidents relating to network and information systems other than those referred to in the preamble of paragraph one, to:

a. organisations which can be considered to objectively have been tasks with informing other organisation or the public about these matters;
b. CSIRTs;
c. other computer crisis teams, designated by decree by Our Minister or belonging to a category which has been designated by means of a directive;
d. providers of internet access and internet communications services for the benefit of informing the users of these services.

3 Furthermore, Our Minister is tasked with: the treatment of voluntary reports as referred to in article 16.

Chapter 3. Other bodies' tasks

Article 4. (competent authority; CSIRT for digital services)

1 The competent authority, as referred to in article 8, paragraph one of the NIS directive, for the sectors is referred to in appendix II of the directive:

Competent authority	***Sector***
Our Minister of Economic Affairs and Climate Policy	power
	digital infrastructure
De Nederlandsche Bank N.V.	banking sector

	infrastructure for the financial market
Our Minister of Infrastructure and Public Works	transportation
	supply and distribution of drinking water
Our Minister for Health, Welfare and Sport	healthcare

2 For the digital services, as set down in annex III of the NIS directive, is:

- **a.** the competent authority, referred to in article 8, paragraph one, of the NIS directive: Our Minister of Economic Affairs and Climate Policy;
- **b.** the CSIRT: the body designated by Royal Decree.

3 The competent authority is obliged to ensure the administrative enforcement of that which has been determined by or under this act with regards to the providers of essential services in the sector or sectors involved, with the exception of the digital services providers.

4 The CSIRT for digital services has the tasks listed in annex I, under 2 of the NIS directive which relate to digital service providers.

Chapter 4. Security demands and reporting incidents

§ 1. General

Article 5. (designating vital providers)

1 In the event of a general order by council or in the event of a resolution by an administrative body listed for that measure, the following will be designated:

- **a.** providers of essential services of categories of these types of providers;
- **b.** other vital service providers or categories of these types of providers.

2 Article 5 and 6 of the NIS directive and annex II of that directive will be adhered to when applying paragraph one, under a.

Article 6. (priority for sector-specific EU regulations)

To the extent article 1, paragraph seven, of the NIS directive applies, it may be determined by general order by council that the designated requirements, resulting from or under this act, do not apply for the designated categories of providers of essential services or digital service providers.

§ 2. Security

Article 7. (risk management)

1 The provider of an essential service and the digital service provider will implement appropriate and proportionate technical measures to manage the risks relating to the security of their network and information systems. These measures will ensure, due to the state of technology, for a level of security which matches the potential risks.

2 The measures referred to in paragraph one applicable to digital service providers will always take the following aspects into account:

- **a.** the security of systems and services;
- **b.** incident handling;
- **c.** the management of operational continuity;
- **d.** supervision, monitoring and testing;
- **e.** adherence to international standards.

Article 8. (preventing incidents and limiting the consequences of incidents)
The provider of an essential service and the digital service provider will implement fitting measure to prevent incidents which affect the security of the network and information systems used by the service in question and to limit the consequences of this type of incident as much as possible with the aim of safeguarding the continuity of that service.

Article 9. (further regulations)
Pursuant to the general management measure, further regulations can be set for the measures referred to in articles 7 and 8.

§ 3. Reporting obligation for incidents

Article 10. (designated vital provider)

1 The vital provider, designated on the basis of article 5, paragraph one, under a or b, will immediately inform our Minister:

- **a.** an incident with significant consequences for the continuity of the services they are making available;
- **b.** a security breach affecting the network and information systems which may significantly affect the continuity of the services they are making available.

2 The provider of an essential service will also immediately report an incident of the type referred to in paragraph one under a, to the competent authority.

3 Without prejudice to article 13, the provider of an essential service will immediately report an incident to Our Minister and the competent authority, if that incident will significantly affect the continuity of the essential services they are providing.

4 To help determine whether or not an incident will have a significant effect on the continuity of an essential service, the following can be taken into account:

- **a.** the number of users affected by the disruption of the service in question;
- **b.** the duration of the incident;
- **c.** the scope of the geographical area affected by the incident.

5 In contrast to article 1, digital service provider is also understood to mean digital service providers who are not under Dutch jurisdiction within the context of paragraph three.

Article 11. (information required as part of a notification)
The notification referred to in article 10 will include the following information:

- **a.** the nature and scope of the incident;
- **b.** the probable time the incident first occurred;
- **c.** the possible consequences both in the Netherlands and abroad;
- **d.** a prognosis of the necessary repair time;
- **e.** if possible, the measures taken by the provider to limit the consequences of the incident or to prevent its recurrence;
- **f.** the contact details of the individual responsible for submitting the notification.

Article 12. (the provision of further details by the designated vital provider)

1 Upon request, the provider submitting a report, as referred to in article 10, paragraph one or three, to Our Minister, will provide all further necessary details requested by Our minister to:

- **a.** offer support to the provider during the implementation of measures to guarantee or restore the continuity of their services;
- **b.** to estimate the risks for the network and information systems referred to in article 3, paragraph one, preamble.

2 The first paragraph will also apply mutatis mutandis if the provider has reported the incident to the competent authority and this party submits the data they have received to Our Minister.

Article 13. (digital service provider)

1 A digital service provider will immediately report an incident which will have a substantial effect on the services they are providing in the European Union to:

- **a.** the CSIRT for digital services, and
- **b.** the competent authority.

2 To help determine whether or not an incident will have a significant effect, as referred to in paragraph one, the following can be taken into account:

- **a.** the number of users affected by the disruption of the service in question;
- **b.** the duration of the incident;
- **c.** the scope of the geographical area affected by the incident.
- **d.** the scope of the disruption to the operation of the service;
- **e.** the scope of the consequences for economical and civic activities.

3 The first paragraph will only apply if the digital service provider has access to the information which is necessary for assessing wether or not the incident will have significant consequences as referred to in that paragraph.

Article 14. (the provision of further details by the digital service providers)

1 Upon request, the digital service provider submitting a notification as referred to in article 13, paragraph one, under a, to the CSIRT for digital services, will immediately provide the CSIRT for digital service with all further details necessary for:

- **a.** offering support to the digital service provider during the implementation of measures to guarantee or restore the continuity of their services;
- **b.** to estimate the risks for the network and information systems belonging to other digital service providers.

2 The first paragraph will also apply mutatis mutandis if the digital service provider has reported the incident to the competent authority and this party submits the data they have received to the CSIRT for digital services.

Article 15. (further regulations applying to the reporting obligation)

Pursuant to the general management measure, further regulations can be set for the measures referred to in articles 10 and 13, including regulations concerning:

- **a.** the data which needs to be provided during the execution of articles 10, 11 and 13;
- **b.** the way in which a report, as referred to in article 10 or 13 is carried out and the way in which the data, as referred to in article 12 is submitted.

§ 4. Voluntary reporting of incidents

Article 16. (the voluntary reporting of incidents)

1 If an incident has significant consequences for the continuity of a service but is not within the scope of the reporting obligation referred in paragraph 3, then the service provider concerned can report that incident to Our Minister.

2 Our Minister will not deal with the notification if it would disproportionately or excessively burden him.

3 Our Minister may submit the notification for processing to:

- **a.** another CSIRT;
- **b.** another computer crisis teams, designated by decree by Our Minister or belonging to a category which has been designated by means of a directive.

Chapter 5. Processing data

Article 17. (data processing by Our Minister or other bodies)

1 Our Minister processes data, including personal data, for the benefit of the goals and tasks listed in article 3. He is controller.

2 The competent authority will process data, including personal data, for the benefit of the goals and tasks listed in article 4, paragraph three. They are the controller.

3 The CSIRT for digital services processes data, including personal data, for the benefit of the goals and tasks referred to in Annex I of the NIS directive. It is the controller.

Article 18. (making data available to Our Minster)

1 Our Minister may request that a legal entity or a body submit data which is necessary for the fulfilment of the tasks listed in article 3, paragraph one, under b up to and including e.

2 The legal entity or body can also make the requested personal data available to our Minister within the context of the first paragraph, if providing this data is incompatible with the purposes for which the personal data was collected.

Article 19. (the provision of incident information to and by the central points of contact)

1 The CSIRT for digital services will inform Our Minister of the notifications received, within the context of article 13, paragraph one, for the execution of article 10, paragraph three, first sentence of the NIS directive.

2 If it becomes clear that a notification submitted by a provider of essential services is an incident within the context of article 10, paragraph one, under a or paragraph three, or article 16, paragraph one, and that
the incident will have significant consequences for the continuity of an essential service in another member state of the European Union, then Our Minister will inform the central point of contact for that member state.

3 At the request of the competent authority or under their own steam, Our Minister will issue the notification referred to in paragraph two to the central point of the contact for the effected member state.

4 Our Minister will contact the central point of contact for the effected member states of an incident, within the context of article 13, paragraph one, which has been reported to the CSIRT for digital services if at least two or more member states have been affected.

5 If it becomes clear from the data received by Our Minister that the central point of contact in another member state that an incident which has been reported there will affect the continuity of:

- **a.** an essential service in the Netherlands: Our Minister will inform the competent authority;
- **b.** a digital service in the Netherlands: Our Minister will inform the CSIRT for digital services and the competent body.

Article 20. (the provision of confidential data by Our Minister)

1 Our Minister will not make confidential data available to a supplier for the execution of the tasks referred to in article 3, if:

- **a.** the privacy of the data is not sufficiently guaranteed, or
- **b.** it is not sufficiently guaranteed that it will only be used for the purposes for which it is being made available.

2 Our Minister can make confidential data available which can be traced to a supplier available without that supplier's permission for the execution of the tasks referred to in article 3, to the extent that this will benefit the measures preventing or limiting the effects of a disruption to society. As a result of the first sentence, data will only be made available to:

- **a.** CSIRTs;
- **b.** other computer crisis teams, designated by decree by Our Minister or belonging to a category which has been designated by means of a directive;
- **c.** the intelligence and security agencies, referred to in the Intelligence and Security Services Act 2017.

3 If a vital provider, or another provider which is part of the national government, does not sufficiently

follow-up on advice issued by Our Minister, then Our Minister can make the data which has been included, as referred to in paragraph two, available to the competent authority or Our Minister concerned.

4 To the extent this is necessary for preventing or limiting serious societal consequences:

- **a.** Our Minister will immediately provide the data referred to in the second article to the competent authority or to Our Minister concerned;
- **b.** Our Minister can, following a consultation with the provider concerned, make the data referred to in paragraph two, available to other organisations or make announcements about this data to the public.

5 The first paragraph does not apply to public notifications referred to in paragraph four, under b.

6 The second paragraph does not apply to the extent necessary for the execution of article 19, paragraphs two up to and including five.

7 The Open Government Law does not apply to the data as referred to in paragraph two, unless and only to the extent that this data contains environmental information as referred to in article 19.1a of the Environmental Management Act. The first sentence also applies to data which resides with another governmental body following a provision within the context of this article.

Article 21. (the provision of confidential data by the CSIRT for digital services)

1 For the execution of the tasks referred to in annex I, under 2 of the NIS directive, the CSIRT for digital services will not issue any confidential data which relates to a digital service provider if:

- **a.** the privacy of the data is not sufficiently guaranteed, or
- **b.** it is not sufficiently guaranteed that it will only be used for the purposes for which it is being made available.

2 For the execution of the tasks referred to in annex I, under 2, of the NIS directive, the CSIRT for digital services can make confidential data available which can be traced to a digital service provider available without their permission, to the extent that this will benefit for the measures preventing or limiting the effects of a disruption to society. As a result of the first sentence, data will only be made available to:

- **a.** CSIRTs;
- **b.** other computer crisis teams, designated by decree by Our Minister or belonging to a category which has been designated by means of a directive;
- **c.** the intelligence and security agencies, referred to in the Intelligence and Security Services Act 2017.

3 If a digital service provider does not sufficiently respond to the advice issued by the CSIRT for digital services, then the CSIRT for digital service may make the data included in the advice, as referred to in the second paragraph, to the competent authority or to Our Minister of Economic Affairs and Climate Policy.

4 The CSIRT for digital services is obliged to immediately provide the data referred to in paragraph two to the competent authority or Our Minister concerned if and to the extent this is necessary for preventing or limiting serious economic or social consequences.

5 The second paragraph does not apply to the extent necessary for the execution of article 19, paragraph one.

6 Article 20, paragraph seven, also applies to the data referred to in article two.

Article 22. (the provision of confidential data by the competent authority)

1 For the execution of the tasks referred to in article 4, paragraph three, the competent authority will not issue any confidential data relating to the provider of an essential service or a digital service provide gained within the context of this act, if:

- **a.** the privacy of the data is not sufficiently safeguarded, or
- **b.** it is not sufficiently guaranteed that it will only be used for the purposes for which it is being made available.

2 Article 20, paragraph seven, also applies mutatis mutandis to the confidential data referred to in paragraph one which can be traced to the provider of an essential service or a digital service

provider.

Article 23. (disclosing incidents)
Without prejudice to article 20, paragraph four, under b, the competent authority may, following a consultation with the provider involved:

- **a.** if public awareness is necessary for the prevention of an incident or for managing an ongoing incident: informing the public about a reported incident as referred to in article 10, paragraph one, under a, or demanding the provider does this;
- **b.** if public awareness is necessary for the prevention of an incident or for managing an ongoing incident, or if disclosing the incident is otherwise beneficial to public interest: informing the public about a reported incident as referred to in article 13, paragraph one, or demanding the digital service provider does this.

Chapter 6. Enforcement

Artikel 24. (scope)
This chapter only applies to the providers of essential services and digital service providers.

Article 25. (regulatory individuals)
1 Those persons designated by a decision of the competent authority are charged with the supervision of compliance with the provisions by and under this law.
2 A decision as indicated in the first paragraph is to be communicated by publication in the Government Gazette.

Article 26. (security audit)
1 The competent authority can, by means of a resolution, oblige the provider of an essential service to:

- **a.** have an independent expert carry out an assessment to determine wether or not the measures implemented by the provider meet the demand made in articles 7 and 8 and the further regulations, as referred to in article 9, and
- **b.** to ensure that the results of that investigation are submitted to the competent authority within a reasonable period of time determined by means of that resolution.

2 The investigation will be carried out in the manner prescribed by the competent authority.
3 Unless an order in council has determined otherwise, the provider will bear the costs of the investigation.
4 Further rules may be laid down with regards to paragraphs one and two pursuant to or under an order in council.

Article 27. (binding designation)
The competent authority can oblige individuals not meeting the demands made in articles 7 or 8 or the further regulations referred to in article 9, by means of instructions to implement the measures described within a reasonable period of time.

Article 28. (administrative enforcement order)
The competent authority is entitled to the imposition of administrative penalties to enforce:

- **a.** that which has been determined by or under this law;
- **b.** article 5:20, paragraph one, of the General Administrative Law Act.

Article 29. (administrative penalty)
1 The competent authority may issue an administrative penalty to the wrongdoer if:

- **a.** that which has been determined by or under this law is violated;
- **b.** that which is stated in article 5:20, paragraph one, of the General Administrative Law Act is violated.

2 The penalty will not exceed:

a. in the event of a violation of article 12, or of article 5:20, paragraph one, of the General Administrative Law Act: 1 million euros;

b. in the event of other violations: 5 million euros.

3 The effect of the decision to implement a fine will be suspended until the appeal period has come to an end or, if an appeal has been submitted, until a decision has been reached concerning the appeal.

4 Protest will suspend the enforcement of an injunction which relates to the collection of the fine.

5 Article 184 of the Criminal Code does not apply to the violation referred to in paragraph one, under b.

Chapter 7. Final Provisions

Article 30. (changes to the General Administrative Law Act)
[Editor: Amends the General Administrative Law Act.]

Article 31. (overlap with the proposal for the Funding of Financial Supervision Act 2019)
[Editor: Changes the Funding of Financial Supervision Act 2019.]

Article 32. (overlap with the Intelligence and Security Services Act 2017)
[Editor: Changes this law.]

Article 33. (overlap with the proposal for the Dutch Open Government Act)
[Editor: Changes the Open Government Act.]

Article 34. (revocation of the Data Processing and Cybersecurity Notification Act)
The Data Processing and Cybersecurity Notification Act is being revoked.

Article 35. (implementation)
This law will come into effect on the date determined by royal decree. A different date may be determined for various articles or parts of articles, for different tasks, or may be open to different interpretation by different categories of providers or services.

Article 36. (short title)
This act shall be known as: Network and Information Systems Act.

Order and command that this shall be placed in the Government Gazette and that all ministries, authorities, bodies, and officials concerned shall diligently keep its execution.

Done at

Wassenaar, 17 October 2018

Willem-Alexander

The Minister of Justice and Security,

F.B.J. Grapperhaus

Published on the eighth of November 2018
The Minister of Justice and Security,

F.B.J. Grapperhaus