

## EUROPEAN NETWORK AND INFORMATION SYSTEMS DIRECTIVE (NISD)

### NIS DIRECTIVE IN GERMANY - IMPLEMENTATION & SPECIFICITIES

March 2021 | Copyright © 2021

#### Current status of implementation

- The German NIS Directive Implementation Act ("Implementation Act") came into effect on 30 June 2017.
- The provisions on providers of digital services are applicable as of 10 May 2018

#### Implementation Act

- The Implementation Act (published in the Federal Law Gazette, BGBl. I 2017 of 29 June 2017, p. 1885) has amended the Act on the Federal Office for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), "FOIS Act"), the Atomic Energy Act (Atomgesetz), the Energy Industry Act (Energie-wirtschaftsgesetz), the Social Security Code V (Sozialgesetzbuch V), and the Telecommunication Act (Telekommunikationsgesetz).
- Due to the amendment of the FOIS Act by the Implementation Act, the FOIS Act now in particular contains a definition of providers of digital services and sets out specific requirements for these providers in connection with security and reporting.
- The key requirements set out in the NIS Directive ("Directive") had, however, already been part of the German IT Security Act ("ITSA") dated 17 July 2015 which amended the FOIS Act before the Implementation Act.

Accordingly, the ITSA had a front-runner role for the Directive. In light of the ITSA, the changes required to German law resulting from the Directive were relatively small.

#### Determination of operators of essential services

- German regulator has specified the criteria to identify operators of the following essential services (Art. 5 NIS):
  - Finance and insurance
  - Energy
  - Health
  - Transportation and traffic
  - IT and telecommunication
  - Water
  - Food

#### Reporting obligations

- There are reporting obligations under certain circumstances:
  - Operators of critical infrastructures must immediately report to the Federal Office for Information Security (FOIS) (i) disruptions [and (ii) significant disruptions] of the availability, integrity, authenticity and confidentiality of their IT systems that have led [might lead] to a failure or significant impairment of the operability of

#### Disclaimer

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. This is a general checklist that will hopefully help your business understand NIS Representative requirement under NISD. It offers a level of minimum requirement and best practise. Cyberlegis RA GmbH does not accept any liability for the correctness of the checklist. You may use this checklist internally in your company. It is not meant to be freely distributed. Any commercial use is forbidden.

the critical infrastructure (Sec. 8b para. 4 of the FOIS Act).

- Providers of digital services (DSP) must immediately report to the FOIS any security incident that has a significant impact on the provision of the digital service provided the EU (Sec. 8c para. 3 of the FOIS Act). The term "significant" is defined in the implementing acts pursuant to Art. 16 para. 8 of NIS Directive. No report is required if the provider does not have sufficient access to information as it may be necessary to evaluate the impact of the security incident.

## Sanctions regime

---

- Fines up to EUR 50.000 (sec. 14 FOIS Act)
- Operators of critical infrastructures wilfully or negligently:
  - fail to properly implement appropriate technical and organisational measures to prevent disruptions of availability etc. in a timely manner;
  - fail to properly designate a point of contact in a timely manner;
  - fail to properly report as described above.
- DSP wilfully or negligently:
  - fail to implement appropriate and proportionate technical and organisational measures to tackle risks for the security of the network and information systems;
  - fail to properly report as described above.
- Infringement of an enforceable ruling: administrative fines up to EUR 100.000
- The administrative fines can run in parallel to fines imposed under the GDPR.
- Infringements of DSPs are only sanctioned by the German authorities, if the DSP
  - has no main establishment in another EU member state;

- as far as the provider has no establishment in another EU member state, the provider has appointed a representative there and offers the digital services in that EU member state.

- Further, the NIS amends the sanction rules under the Atomic Energy Act, Energy Industry Act, Social Security Code V and Telecommunication Act, whilst the administrative fines remain as before:

- Up to EUR 50.000 under the Atomic Energy Act;
- Up to EUR 5.000.000, or in specific cases up to 10% of the total worldwide annual turnover of the preceding financial year, under the Energy Industry Act;
- Up to EUR 50.000 under the Social Security Code V; and
- Up to EUR 500.000 under the Telecommunication Act.

## Competent authorities

---

- Information security on a national level, including the prosecution and control of administrative offences: FOIS
- The FOIS operates under the authority of the German Federal Ministry of the Interior.

## Jurisdictional applications

---

- Operators of critical infrastructure are subject to German law if the infrastructure is located in Germany.
- Reporting obligations do not apply to DSPs that have their main establishment in another EU member state or have appointed a Rep in another EU member state, in which they offer the digital services.
- Other obligations apply to providers even though their main establishment is outside of Germany.

### Disclaimer

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. This is a general checklist that will hopefully help your business understand NIS Representative requirement under NISD. It offers a level of minimum requirement and best practise. Cyberlegis RA GmbH does not accept any liability for the correctness of the checklist. You may use this checklist internally in your company. It is not meant to be freely distributed. Any commercial use is forbidden.

## About Us

---

- Cyberlegis RA GmbH (**CYBERLEGIS**) is a an European Tech Data Law Firm in Munich.
- CYBERLEGIS specializing in NIS Representative Services under NISD.

## Why hire CYBERLEGIS as your NIS Representative?

---

- **EFFICIENCY:** CYBERLEGIS is a specialized provider for representative services. CYBERLEGIS works on your request within 6 hours.
- **COST EFFECTIVE:** At just EUR 1.200 net per year CYBERLEGIS provides premier EU representation services.
- **INSURANCE COVERAGE:** Since all NIS Representatives installed by CYBERLEGIS are specialized Privacy lawyers, the service comes along with a default liability of 1 Million Euros (with higher representation available at extra cost).
- **PROFESSIONALISM:** CYBERLEGIS is sensitive to providing quality service to its clients. Thus, CYBERLEGIS designates only specialized Experts to act as NIS Representatives or handle representation-related matters for the clients.



No set up fees



A Compliant NIS REP agreement



Yearly NISD report



Contact by Tel/Fax/E-mail



Secretary answering phone calls



Local authority contacts



Experienced privacy attorneys



Access to our help-desk

- **ASSURED AVAILABILITY:** In an effort to satisfy its clients, the designated NIS Representative would be reachable not only from Monday to Friday (09:00h – 17:00h) via a team of English speaking secretaries, but equally at weekends via e-mail and cell phone.
- CYBERLEGIS has minimum 3 legal experts, working around the clock to assist the clients fulfil the NISD requirements. Thus, at any given point in time, a CYBERLEGIS representative is always there to assist you with your requirements.

## How do I designate CYBERLEGIS as my EU Representative?

---

- Just email us at: [niedermeier@cyberlegis.io](mailto:niedermeier@cyberlegis.io) and we will be happy to answer all your question in a Zoom or WebEx meeting.
- We have standard document designating one of our expert Lawyers as your NIS Representative. In this regard, you would receive a draft designation document, which you would print, sign, and send by post, in accordance with NISD.
- Please connect with "RA Robert Niedermeier" on LinkedIn:  
[www.linkedin.com/in/ra-robert-niedermeier](https://www.linkedin.com/in/ra-robert-niedermeier).  
Robert Niedermeier CIPP/E CIPT CIPM FIP (Mobile +49 171 2440099).

### Disclaimer

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. This is a general checklist that will hopefully help your business understand NIS Representative requirement under NISD. It offers a level of minimum requirement and best practise. Cyberlegis RA GmbH does not accept any liability for the correctness of the checklist. You may use this checklist internally in your company. It is not meant to be freely distributed. Any commercial use is forbidden.

**Disclaimer**

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. This is a general checklist that will hopefully help your business understand NIS Representative requirement under NISD. It offers a level of minimum requirement and best practise.

Cyberlegis RA GmbH does not accept any liability for the correctness of the checklist. You may use this checklist internally in your company. It is not meant to be freely distributed. Any commercial use is forbidden.