

NIS 2 Compliance by manufacturers of medical devices

Addressees and measures necessary for compliance with the new EU Directive on cybersecurity

The new Network and Information Security Directive (NIS 2 Directive) significantly tightens the cybersecurity requirements for manufacturers of medical devices. The new requirements must be applied by the EU Member States by 18 October 2024 at the latest.

Who is addressed?

The Directive addresses manufacturers with 50 or more employees or an annual turnover and an annual balance sheet total of 10 million euros, that manufacture medical devices within the meaning of Art. 2 (1) of the EU Regulation on medical devices. This includes, amongst others, the manufacture of instruments, apparatus, appliances, software, implants or other articles intended to be used for human beings for one of the following specific medical purposes:

- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease;
- diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability;
- investigation, replacement or modification of the anatomy or of a physiological or pathological process or state.

What is to be implemented?

The requirements of the NIS 2 Directive can be grouped into three categories. The first category concerns the area of governance and awareness. The management must take and monitor cybersecurity measures. Managing directors are personally liable in the event of breaches. The second category covers

the management of cybersecurity risks. Identified risks must be made manageable through technical and organisational measures. Cybersecurity must also be guaranteed in the supply chain. The third category of requirements includes reporting obligations towards the supervisory authorities.

What to expect in the case of breaches?

The competent supervisory authorities can carry out on-site inspections and targeted security audits. In the event of breaches, there is a risk of high fines and public warnings in addition to orders from the supervisory authority.

Our services

We support you in implementing the requirements of the NIS 2 Directive by rendering, amongst others, the following services:

- Legal review and consideration whether your company is addressed by the Directive
- Derivation of specific cybersecurity requirements and gap analysis
- Legal support in the implementation and documentation
- Establishment of a cybersecurity compliance managements

Next step: Get in touch

We would be pleased to explain our approach to you in a personal meeting.

T +49 30 / 2332 895 0

E info@reuschlaw.de