Denmark

Your local contact

Aleksandar Predrag Piletich
Head of Privacy, Data Protection & Cyberlaw
Director, PwC Denmark
+45 2928 5743
aleksandar.predrag.piletich@pwc.com

Status	Transposed into national law and came into force on 1 July 2025.
Name of National Law	In Danish: Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS-2-loven) In English: Act on measures to ensure a high level of cybersecurity (the NIS-2 Act)
Entered into force	The NIS-2 Act entered into force on 1 July 2025. The NIS-2-Directive has been transposed into separate legislation for the energy, telecom, and financial sectors. • Energy: In force since 7 March 2025. Also implements the CER Directive. • Telecom: In force since 1 July 2025. • Finance: Aligned with the DORA Regulation. In force.
Link to current draft or equivalent	https://www.retsinformation.dk/eli/lta/2025/434
Scope (deviating from NIS-2-Directive)	• **Size criteria**: An entity must meet at least one of the following criteria: a) Employ 50 or more persons; or b) have an annual turnover exceeding EUR 10.000.000 and an annual balance sheet total exceeding EUR 10.000.000. The criteria are not cumulative, meaning companies with 50 employees are subject to NIS-2 - provided they operate within Annex I and/or II - regardless of turnover or balance sheet total. • **Public sector**: All public administrative bodies are generally covered, including municipalities. However, the Danish Parliament (Folketinget), the National Audit Office, the Parliamentary Ombudsman, and the courts are excluded, as are certain educational and cultural institutions that do not exercise significant public authority, and unemployment insurance funds, as they are not subject to the Public Administration Act. Public authorities involved in national and public security, defense, or law enforcement are exempt from the NIS-2 Act. • **Chemicals**: (not explicitly stated in the NIS-2 Act) Entities engaged in the manufacture, production, or distribution of chemicals are not considered within the scope of the NIS-2 Act if they are not subject to the registration requirement for hazardous industrial chemicals under REACH. • **Energy**: The energy sector is subject to specific thresholds that vary depending on the sub-sector and type of entity. Depending on the risk classification, additional and stricter requirements may apply. • **Telecom**: Providers with limited activity are exempt from most NIS-2 requirements (e.g. cafés, hotels, housing associations, gas stations, shopping centers). In other words, if telecom services are offered for commercial purposes but are not the entity's primary activity - or are merely an accessory - these entities are generally not subject to the NIS-2.
Registration	Although the NIS-2 Act came into force on 1 July 2025, a transitional provision extends the registration deadline, requiring covered organizations to register by 1 October 2025. Registration is done via Single Point of Contact (Virk.dk) using MitID - available from 1 July 2025 - where you can select the relevant sectoral authority listed here.

Denmark

Information Security Standards referenced	The NIS-2 Act does not reference specific standards. However, official guidance mention, among others, DS/EN ISO/IEC 27001:2023, NIST Cybersecurity Framework (CSF) 2.0, DS/IEC 62443-2-1:2011, DS/EN IEC 62443-3-3:2019 etc.
Incident reporting	No deviations from the NIS-2-Directive. Incidents with significant impact under NIS-2 and data breaches under GDPR can be reported through the same process and online platform.
Authority / CSIRT	Reports are handled by the Danish Defence Intelligence Service, which serves as the national CSIRT.
Fines (deviating from NIS-2-Directive)	• **No administrative fines**: The legal systems of Denmark do not allow for administrative fines. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty. Therefore, the competent national courts should consider the recommendation by the supervisory authority initiating the fine.
Worth mentioning	The telecom, energy, and financial sectors, which are not subject to the main NIS-2 Act but are instead regulated separately, are already subject to sector-specific cybersecurity legislation. As a result, these laws contain more specific requirements than the main NIS-2 Act and, in some cases, even stricter obligations.

Your local contact

Aleksandar Predrag Piletich
Head of Privacy, Data Protection & Cyberlaw
Director, PwC Denmark
+45 2928 5743
aleksandar.predrag.piletich@pwc.com