NEWSLETTER

The Danish NIS2 Act has entered into Force: **Board Liability Strengthened**

Moalem Weitemeyer

Introduction

Denmark's NIS2 Act (Act No. 434 of 6 May 2025) entered into force on 1 July 2025, implementing the EU NIS2 Directive.

The Act represents a major shift in the regulation of cybersecurity for both public and private entities in Denmark and across the Nordic region.

The purpose of the Act is to ensure a high, common level of cybersecurity across sectors, from energy and transport to healthcare, food, digital infrastructure, and research.

It applies to both "essential entities" (typically major operators and public bodies) and "important entities" (medium-sized companies and suppliers in critical supply chains).

New Obligations for Boards and Management

Section 7 of the NIS2 Act introduces an explicit responsibility for boards of directors and executive management with respect to cybersecurity.

The management body must:

- Approve the technical and organizational measures adopted to manage cyber risks (Section 6).
- Supervise the implementation and continuously assess the effectiveness of such measures.
- Participate in relevant training on cybersecurity risk management and ensure that similar training is provided to employees.

Failure to comply may lead to regulatory action, fines, and, in serious cases, temporary suspension of management members (Sections 22-23 and 32). This strengthens the existing duty of care under Section 115 of the Danish Companies Act.

A Heightened Threat Environment

According to the Danish Defence Intelligence Service and the Centre for Cyber Security, the cyber threat level against Danish authorities and companies remains “very high”.

Hybrid attacks increasingly combine cyber intrusions, physical sabotage, and disinformation, particularly targeting the energy, water, and critical infrastructure sectors.

The new legislation has been designed precisely to address this convergence of digital and physical threats

What Boards should do now

1. Establish governance structures: Appoint responsible cybersecurity officers and ensure formal board-level oversight.

2. Update policies and contingency plans: Review risk management, incident response, supplier security, and business continuity in light of Section 6.

3. Document decisions: Ensure approval, monitoring, and follow-up are properly recorded in board minutes.

4. Implement training: Schedule mandatory cybersecurity training for directors and executives by the end of 2025.

5. Prepare for supervision: Ensure compliance documentation is ready for submission to competent authorities upon request.

Our Comments

Cyber and operational resilience are no longer merely technical issues; they are matters of legal governance.

The NIS2 Act establishes a new baseline for cybersecurity compliance in Denmark, requiring boards to demonstrate informed, active, and documented oversight.

Timely action is now essential. Not only to avoid sanctions but to safeguard critical business operations in an increasingly complex threat landscape.

Contacts

Thomas Mygind

Partner

thomas.mygind@moalemweitemeyer.com

Kevin Lerbech Formann Kristensen

Associate

kevin.kristensen@moalemweitemeyer.com

Jacob Kreutzmann

Associate

jacob.kreutzmann@moalemweitemeyer.com