NIS2 Directive finally implemented in Poland

What businesses need to know

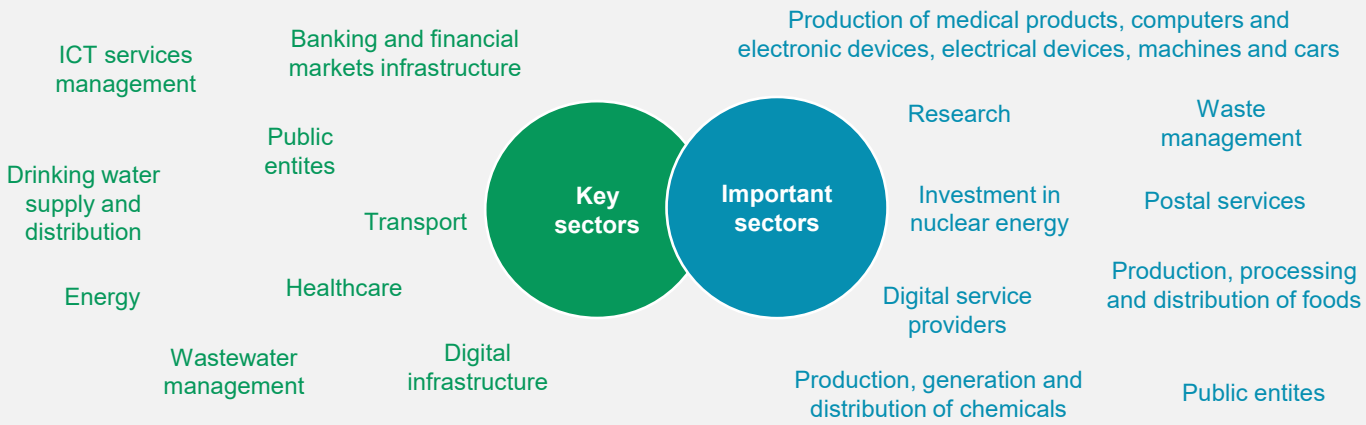
On 19 February 2026, the President of Poland signed the amendment to the National Cybersecurity System Act ("**UKSC**"), implementing Directive (EU) 2022/2555 ("**NIS2 Directive**") in Poland. Presidential signature marks the final legislative step before the new regime enters into force.

The law will enter into force following a one-month *vacatio legis* from its publication in the official journal of laws (so the law will become applicable in early April 2026).

For businesses operating in Poland, this signals **a shift from legislative monitoring to active implementation and the need to effectively start a regulatory compliance journey.**

KEY REGULATORY CHANGES COMPARED TO THE NIS1 REGIME:

- Replacement of the previous classification of operators of essential services and digital service providers with 'essential entities' and 'important entities'.
- Significant expansion of sectors covered, including not only energy, transport, healthcare and banking, but also food production and distribution, chemicals, postal and courier services, waste management, digital infrastructure and the space sector. The full list of sectors is visible below:



- Strengthened supervisory powers, including the ability to order security audits and issue binding instructions in response to incidents.
- Creation of sectoral CSIRTs to support incident response and coordination.
- Enhanced obligations for management boards and personal liability, including mandatory documented training.

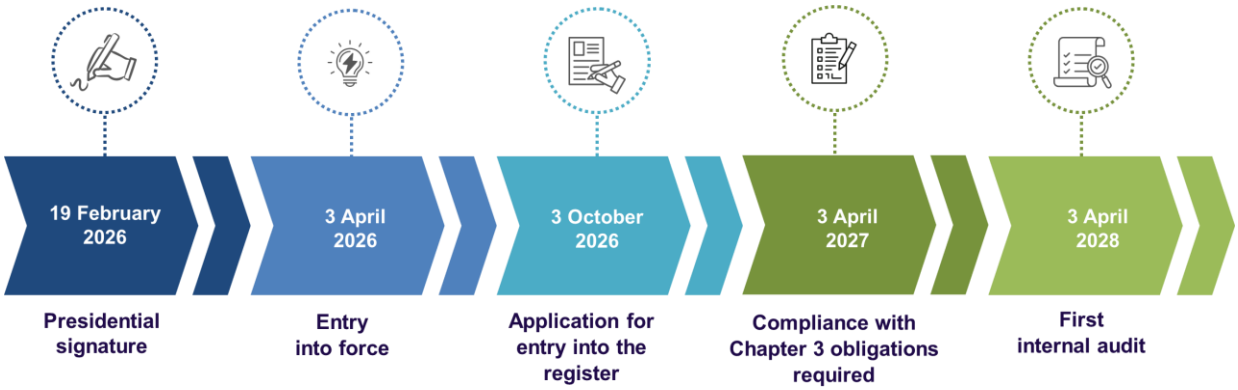
ADDLESHAW GODDARD

NIS2 Directive finally implemented in Poland

What businesses need to know

IMPLEMENTATION TIMELINE

1. 19 February 2026 – Presidential signature.
2. 3 April 2026 – Entry into force (following one-month *vacatio legis*).
3. 3 October 2026 – submission of an application for entry into the official register of essential and important entities.
4. 3 April 2027 – essential and important entities must implement and comply with the obligations set out in Chapter 3 of the UKSC.
5. 3 April 2028 – the first audit must be carried out by entities which, on the date of entry into force of the UKSC, meet the criteria for recognition as a key entity.



FIRST STEP – SELF ASSESSMENT

Businesses should now transition from the stage of analysing potential changes to the stage of implementing new rules under the amended UKSC. The starting point should be a self-assessment by the business to determine whether it qualifies as a key entity or an important entity within the meaning of the UKSC. This assessment may be complex and require an analysis of sector classification, size thresholds, and the nature of the services provided.

COMPLIANCE STEPS

Entities falling into scope of the UKSC will need to take the following steps:

- implementation of risk-appropriate technical and organisational measures tailored to scale, services and risk profile;
- review and test incident detection and reporting mechanisms;
- comprehensive supply chain review, including potential exposure to technology suppliers designated as ‘high-risk’;
- ensure documented management oversight of the area of cybersecurity;
- alignment of UKSC compliance with overlapping regimes, e.g. DORA, GDPR and other EU digital regulations.

ADDLESHAW GODDARD

NIS2 Directive finally implemented in Poland

What businesses need to know

SANCTIONS AND ENFORCEMENT EXPOSURE

Failure to comply with UKSC may result in severe, GDPR-alike financial penalties. As a general rule:

- **Essential entities** may be subject to administrative fines of up to EUR 10 million (approx. PLN 42.4 million) or 2% of the total worldwide annual turnover, whichever is higher;
- **Important entities** will face fines of up to EUR 7 million (approx. 29,4 million) or 1.4% of the total worldwide annual turnover, whichever is higher.

UKSC also provides for fines of up to **PLN 100 million** where it is determined that an essential or important entity has breached UKSC and, at the same time, caused a direct and serious cyberthreat to national defence, state security, public safety and order, or human life and health; or has created a risk of significant financial damage or serious disruption in the provision of services.

MANAGEMENT BOARD LIABILITY

The UKSC introduces a model of enhanced liability for the management of essential and important entities and reinforces cybersecurity as an area requiring oversight at the level of the management board. The head of an essential or important entity, which in the case of companies will typically be the management board, is required to ensure the implementation and effective oversight of cybersecurity risk management measures and to ensure the entity's compliance with its obligations under the UKSC.

The management will therefore bear direct responsibility for fulfilling obligations under the UKSC. The UKSC provides for financial penalties for management for breaches of obligations arising from the Act.

The UKSC also introduces a mandatory requirement for regular training of the management board and expressly excludes the possibility of shifting responsibility for cybersecurity tasks to lower levels within the organisation. In light of the expanded supervisory powers and the significant level of sanctions, cybersecurity must be subject to genuine and documented oversight at the level of the management board of entities falling within the scope of the UKSC.

HOW CAN WE HELP?

We advise businesses on mapping and implementing obligations arising under NIS2 Directive (on EU-wide level) and the amended UKSC in Poland. We suport our Clients in particular in:

- assessing whether the new NIS2 Directive/UKSC obligations apply to your organisation;
- identifying the specific regulatory requirements;
- implementing cybersecurity policies, procedures and documentation;
- advising on the legal aspects of cybersecurity incident management and reporting;
- reviewing agreements with ICT product and service providers;
- delivering training for management boards and IT teams on the new regulatory requirements.

CONTACT

SZYMON SIENIEWICZ
Counsel
Head of TMT/IP
Tel +48 22 526 5042
Mob +48 665 052 724
szymon.sieniewicz@aglaw.com

ADDLESHAW GODDARD