Clifford Chance

BRIEFING

Poland: Delayed Implementation of the NIS2 Directive

3 March 2026 r.

On 19 February 2026, the President Karol Nawrocki signed an amendment to the Act on the National Cybersecurity System (the "Amendment" and the "Cybersecurity Act"). This Amendment is designed to implement the NIS2 Directive[1] and it will come into force on 2 April 2026.

At the same time, the President has referred the Amendment to the Constitutional Tribunal for subsequent review of some of its provisions, including those on high-risk providers, security orders, and administrative penalties. If the Tribunal finds these provisions unconstitutional, they will no longer apply.

Expansion of the List of Entities Covered by the Cybersecurity Act

Be The previous categories – operators of essential services and digital service providers – have been replaced with two new groups: important entities and key entities. At the same time, the range of sectors covered by the Cybersecurity Act has been broadened.

Earlier, the Cybersecurity Act applied to the following sectors:

- Energy
- Transport
- Banking and financial market infrastructure
- Healthcare
- Drinking water supply and distribution
- Digital infrastructure

With the recent Amendment, the Cybersecurity Act now covers two categories of sectors:

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

- **Key Sectors**
    - Energy
    - Transport
    - Banking and financial market infrastructure
    - Health
    - Drinking water supply and distribution
    - Collective sewage disposal
    - Digital infrastructure
    - ICT service management
    - Space
    - Public administration
- **Important Sectors**
    - Postal and courier services
    - Nuclear energy investments
    - Waste management
    - Manufacture, production and distribution of chemicals
    - Production, processing and distribution of food
    - Manufacturing
    - Research
    - Public entities, including local government units and budgetary institutions.

Different Regulators and CSIRTs for Each Sector

The amended Cybersecurity Act continues to assign regulatory responsibilities to different authorities based on the sector involved. Depending on the sector, the relevant regulator may be a government minister, the Polish Financial Supervision Authority or the President of the Office of Electronic Communications.

In addition to the existing Computer Security Incident Response Teams (CSIRTs), new sector-specific CSIRTs will be set up. These teams aim to strengthen the response to cyber threats and help build a sector-specific knowledge base on risks and vulnerabilities. For example, in October, the Ministry of Digital Affairs announced the creation of CSIRT Cyfra, a dedicated CSIRT for the digital infrastructure sector.

Criteria for Being Classified as a Key or Important Entity

Key Entities

Entities considered essential include:

- entities operating in a Key Sector that employ at least 250 people, have an annual turnover of more than EUR 50 million or a balance sheet total exceeding EUR 43 million.
- electronic communications undertakings that employ at least 50 people, have an annual turnover or balance sheet total exceeding EUR 10 million.
- managed cybersecurity service providers that employ at least 10 people and whose annual turnover or balance sheet total exceeds EUR 2 million.

- certain other entities regardless of size, such as operators of nuclear facilities, DNS service providers, domain name registration service providers and critical entities.

Important Entities

Important entities include among others:

- entities operating in Key Sector that employ at least 50 but fewer than 250 people, or has an annual turnover of up to EUR 50 million or a balance sheet total of the equivalent of more than EUR 10 million but not exceeding the equivalent of EUR 43 million.
- entities operating in Important Sector that employ at least 50 people or has an annual turnover or balance sheet total of the equivalent of more than EUR 10 million.

Procedure for Entry into the Register – Self-Identification Requirement

Each organisation must assess for itself whether it meets the criteria to be classified as a key or important entity. If it does, it must submit an electronic application to the Register of Key and Important Entities (the "**Register**").

The Register should be established by the minister responsible for computerisation (currently the Minister of Digital Affairs) within one month of the Amendment coming into effect.

Entities already listed in the existing register of key service operators will be added to the new Register automatically by the minister. The minister will also publish a timetable for submitting applications for entry into the Register for organisations that meet the criteria for key or important entities when the Amendment takes effect and begin using the ICT system (S46).

Applications for entry into the Register must be submitted within six months of meeting the legal requirements for recognition as a key or important entity. If there are any changes to the information in the Register, an application to update the entry must be submitted within 14 days of the change.

The regulator for each sector also has the power to designate an organisation as a key or important entity and add it to the Register if it has not registered itself.

Key Obligations

Beyond the requirement to apply for entry in the Register, key and important entities must comply with several additional obligations.

As part of their information security management systems, entities must:

- Implement advanced cybersecurity measures
- Establish a risk assessment policy
- Ensure the security of the ICT supply chain (covering products, services and processes)
- Continuously monitor their systems
- Provide cybersecurity training for employees
- Identify cyber threats
- Analyse their resources

- Review existing procedures
- Introduce effective incident response procedures.

The specific obligations may differ depending on the sector in which the entity operates. The extent of these measures should be tailored to the size of the organisation and its level of risk exposure.

Additional responsibilities include:

- Appointing at least two people responsible for maintaining contact with national cybersecurity system entities
- Enabling users to report cyber threats or incidents related to the services provided
- Expanding documentation related to information system security
- Changing the procedure for reporting serious incidents (i.e. events that cause, or could cause, significant service disruption, major material or non-material damage, or significant financial losses).

Incident Reporting

A new multi-stage process for reporting serious incidents has been introduced, using the ICT system (S46). Serious incidents are defined as events that significantly disrupt, or could disrupt, the continuity of service provision, cause financial losses or result in serious harm to users.

The reporting process includes the following steps:

- **Early warning:** Must be submitted immediately, and no later than 24 hours after detecting the incident, to the relevant sectoral CSIRT.
- **Serious incident report:** Must be submitted immediately, and no later than 72 hours after detection, to the relevant sectoral CSIRT.

If a serious incident occurs, a final report must be submitted within one month of the initial report, using the S46 system. This final report should include a description of the incident, actions taken, an analysis of the effects (including any cross-border impact), and an assessment of the causes. In certain cases, the relevant CSIRT may also request periodic updates on how the incident is being managed.

Key and important entities have six months from the date the Cybersecurity Act comes into force to update their serious incident reporting procedures to comply with these new requirements.

Transitional Period for Fulfilling Obligations

Key or Important Entities

Organisations that meet the criteria for key or important entities on the date the Amendment comes into force must begin implementing the requirements of the Cybersecurity Act within 12 months. This includes setting up an information security management system, preparing documentation, establishing incident response procedures, creating cybersecurity structures and appointing contact persons.

Key entities must also carry out their first cybersecurity audit within 24 months of the Amendment coming into force. After this, audits must be conducted regularly, at least once every three years (previously, audits were required every two years).

Existing Operators of Key Services

For six months after the Amendment comes into force, existing operators of key services should continue to report serious incidents using the current procedure.

Telecommunications Operators

Until the new obligations under the Amendment are in place, telecommunications operators must continue to comply with their existing duties under the Telecommunications Law.

Entities Recognised as Key or Important by Administrative Decision

If an organisation is designated as a key or important entity by a competent regulator's administrative decision, the deadlines – 12 months for implementing the new obligations and 24 months for the first audit – will be counted from the date the decision is delivered.

Administrative Penalties and Transition Period

Key and important entities may face financial penalties if they fail to meet specific cybersecurity obligations.

The level of penalty depends on the entity's status:

- **Key entities:** The maximum penalty is EUR 10,000,000 or 2% of revenue from the previous financial year, whichever is higher, but not less than PLN 20,000.
- **Important entities:** The maximum penalty is EUR 7,000,000 or 1.4% of revenue from the previous financial year, whichever is higher, but not less than PLN 15,000.

For the most serious breaches – those that create a direct and serious cyber threat to national defence, state security, public safety and order, human life or health, or that risk serious property damage or major disruption to services – the penalty can be as high as PLN 100,000,000, regardless of the entity's status.

Personal Liability of Management

The Amendment introduces personal liability for managers of key entities if certain obligations are breached. This applies to individuals such as management board members, partners managing a partnership, liquidators, receivers or administrators in restructuring proceedings, and succession administrators.

Personal liability may arise in connection with breaches relating to:

- Entry into the Register and keeping information up to date
- Decisions about preparing, implementing, applying, reviewing, and supervising the entity's information security management system
- Allocating sufficient financial resources to meet cybersecurity obligations
- Assigning and supervising cybersecurity tasks
- Ensuring staff are aware of cybersecurity duties and understand internal regulations

- Ensuring the entity's operations comply with the law, including the Amendment and internal regulations
- Completing annual mandatory cybersecurity training for both the manager and any person acting on their behalf
- Handling incidents.

Penalties for managers may be:

- Up to 300% of the manager's remuneration (calculated according to the rules for holiday pay) for key or important entities
- For public entities, up to 100% of the manager's remuneration calculated in the same way.

Multiple Managers

If a key or important entity is managed by a multi-member body (e.g. a management board), all members are liable for compliance with the obligations, unless a specific individual has been designated as responsible for a particular area under the Cybersecurity Act.

Suspension of Penalties

Except for the most serious breaches (which can result in penalties of up to PLN 100,000,000), penalties for non-compliance may only be imposed two years after the Amendment comes into force.

If an infringement is identified before this two-year period ends, no penalty will be imposed at that time. However, the law does not rule out the possibility of penalties being applied for breaches that occurred during this period, once the two years have passed.

As a result, there is some uncertainty, but it is likely that the next two years will be treated as a transitional period. During this time, undertakings will not be penalised for non-compliance with the new requirements, provided they remedy any breaches within two years of the Amendment taking effect.

Procedure for Identifying High-Risk Suppliers

A new procedure to identify high-risk suppliers will support the implementation of the requirement for supply chain security. It will help prevent equipment and services that do not meet cybersecurity standards from entering the market. The Minister of Digital Affairs will make decisions on high-risk suppliers, after consulting the College for Cybersecurity. Suppliers who disagree with such a decision can appeal to an administrative court.

Key points include:

- Entities essential to the functioning of the state are prohibited from introducing products from high-risk suppliers into their systems. If they are already using such products, they must remove them within seven years of the decision being issued.
- Suppliers from outside the EU and NATO will not automatically be classified as high-risk. Entities using equipment or software from these suppliers will not be required to suspend their activities in connection with the withdrawal obligation.
- The decision of the Minister of Digital Affairs will apply only to the specific equipment or software named in the decision, not to all products from the supplier. Only the identified equipment or software will need to be withdrawn.

New Powers for Cybersecurity Authorities

The Amendment increases the powers of authorities responsible for cybersecurity, enabling a faster and more effective response to threats. Sector-specific authorities responsible for cybersecurity – such as government ministers, the Polish Financial Supervision Authority and the President of the Office of Electronic Communications – will be able, among other things, to issue warnings, appoint monitoring officials and order security audits and assessments.

Key changes include:

- The Minister of Digital Affairs will have new powers to issue security orders during critical incidents and to lead educational initiatives on cybersecurity.
- The Government Plenipotentiary for Cybersecurity will be able to issue recommendations, request information from administrative bodies, commission necessary research and purchase software for participants in the Joint Cybersecurity Operations Centre.
- National CSIRTs, including CSIRT NASK, will have new responsibilities to support an increasing number of key and important entities in managing incidents. The Joint Cybersecurity Operations Centre will be introduced into the Cybersecurity Act as the central point for sharing information on cyber threats, incidents and vulnerabilities.

Improvement of the incident reporting procedure

Information about reported incidents will be forwarded directly to CSIRTs, with direct communication enabled by the new S46 system developed by the National Research Institute (NASK-PIB) on the instructions of the Minister of Digital Affairs (the owner of the system). Entities will gain access to S46 after being entered into the Register.

Inclusion of a Representative of the President in the Development of an Incident Response Plan

The participation of the President's representative in the work on the National Plan for Responding to Incidents and Crisis Situations in Cybersecurity has been included, which is intended to strengthen cooperation between key state institutions. The national plan, developed by the Minister of Digital Affairs in cooperation with, among others, the Government Centre for Security and the President's representative, will be adopted by the Council of Ministers.

Improvement of the Incident Reporting Procedure

Reported incidents will now be communicated directly to CSIRTs through the new S46 system. This system, developed by the National Research Institute (NASK-PIB) for the Minister of Digital Affairs, the owner of the system, enables direct and efficient communication. Entities will be granted access to the S46 system once they are entered in the Register.

Inclusion of a Presidential Representative in Incident Response Planning

A representative of the President will now participate in developing the National Plan for Responding to Incidents and Crisis Situations in Cybersecurity. This aims to enhance cooperation between key state institutions. The national plan, prepared by the Minister of Digital Affairs in

collaboration with, among others, the Government Security Centre and the President's representative, will be adopted by the Council of Ministers.

Summary

The Amendment greatly broadens the range of entities subject to regulation and introduces new, stringent cybersecurity obligations. These include comprehensive IT risk and security management procedures, new incident reporting requirements and measures for identifying and managing high-risk suppliers. Supervisory authorities have been granted stronger powers, and the Amendment introduces severe penalties, including personal liability for management. As a result, organisations must quickly adapt their processes to meet the new requirements to ensure operational security and reduce regulatory risks.

The Amendment goes beyond the minimum standards set by the NIS2 Directive. Its extensive obligations for undertakings and the wide-ranging rights and discretionary powers given to regulators have attracted criticism from some in the business community.

To fully assess the Amendment's impact on businesses, it will be important to monitor the introduction and application of implementing regulations, as well as how regulators enforce the Cybersecurity Act in practice.

Agnieszka Janicka
Partner, Warsaw

E:agnieszka.janicka@clifffordchance.com
T: +48 22 627 11 77

Krzysztof Hajdamowicz
Counsel, Warsaw

E:krzysztof.hajdamowicz@cliffordchance.com
T: +48 22 627 11 77

Martyna Sieczka
Advocate Trainee, Warsaw

E:martyna.sieczka@cliffordchance.com
T: +48 22 627 11 77

cliffordchance.com

ul. Lwowska 19, 00-660 Warsaw, Poland

Akta rejestrowe przechowuje Sąd Rejonowy dla m.st. Warszawy w Warszawie XII Wydział Gospodarczy Krajowego Rejestru Sądowego KRS: 0000053301 NIP: 5262579191