SOŁTYSIŃSKI KAWECKI SZLĘZAK

Legal cybersecurity standards – major changes are coming

In the coming days, Polish regulations introducing a range of cybersecurity obligations will enter into force. **The new rules will expand both the group of entities subject to cybersecurity obligations and the scope of those obligations.**

Existing solutions in this area have proved to be inadequate. At the European Union level, the NIS 2 Directive[1] has been adopted, leading to an amendment to the National Cybersecurity System Act (NCS Act).

The new regulations are intended to be a step towards digital security for both the private and public sectors. This means an investment that will involve additional financial outlay and obligations. Who in the organization should deal with cybersecurity? When will the new rules enter into force? Who will be covered by them? What obligations and sanctions will they introduce? Should you prepare, and if so, where should you start? The answers to these and other questions can be found in this article.

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 (the NIS 2 Directive).

Management Boards will be responsible for cybersecurity obligations

Responsibility for fulfilling cybersecurity obligations has been imposed on the managers of entities covered by the Act (the Act provides for two categories of entities, i.e., essential and important, which are discussed below). Where an essential or important entity is managed by a multi-member body; all members of that body will be held responsible unless a specific person has been designated.

NOTE: The manager of an essential or important entity will also be held responsible where some or all obligations are delegated to another person. The explanatory memorandum to the Act clearly emphasizes that the purpose of these solutions is to ensure that an entity's management takes the provision of the entity's cybersecurity seriously.

Managers of essential and important entities will be responsible for fulfilling specific obligations, including making decisions on the preparation, implementation, application, and review of the entity's information security management system, as well as ensuring that adequate financial and human resources are planned for to carry out cybersecurity obligations. In addition, they will be required to attend cybersecurity training once a year.

NOTE: If statutory obligations are not fulfilled, the authority will be able to impose a financial penalty on the entity's manager of up to three times their remuneration and may even prohibit them from performing managerial functions until the infringements cease.

Who is a manager?

- members of the management board or another management body
- partners managing a company's affairs in a registered partnership and in a civil-law partnership
- partners managing a company's affairs, or the management board, in a professional partnership
- general partners managing a company's affairs in the case of a limited partnership, and for a limited joint-stock partnership, the general partners managing the company's affairs
- natural persons engaged in business

Key dates

- **n –** the date of publication in the Journal of Laws
- **n + 1 month –** the Act enters into force
- **n + 7 months** – deadline for self-registration by important and essential entities
- **n + 13 months** – deadline to comply with the requirements of the Act
- **n + 25 months** – deadline to carry out the first audit for new essential entities
- **n + 25 months –** period during which the authority will not impose penalties for certain failures to meet obligations

Who will be covered by the new regulations?

The new regulations introduce a division of entities covered by the Act into essential and important entities.

It is for the entities covered by the Act to verify whether they qualify for one of these categories. Two criteria are decisive: size (as a rule, at least medium-sized enterprise status) and the scope of the activities carried out.

Scope of activities

An annex to the Act describes the types of activities which may result in an entity being classified as essential or important.

NOTE: The assessment must take into account all types of activities carried out by the entity. In some cases, ancillary activities — or activities negligible from a revenue perspective — may determine that the entity must comply with the Act's requirements.

ESSENTIAL SECTORS

- ENERGY
- TRANSPORT
- BANKING
- FINANCIAL MARKET INFRASTRUCTURES
- HEALTHCARE
- DRINKING WATER SUPPLY AND DISTRIBUTION
- WASTE WATER
- DIGITAL INFRASTRUCTURE
- ICT SERVICE MANAGEMENT
- PUBLIC ADMINISTRATION
- SPACE

IMPORTANT SECTORS

- POSTAL AND COURIER SERVICES
- WASTE MANAGEMENT
- PRODUCTION, MANUFACTURE, AND DISTRIBUTION OF CHEMICALS
- PRODUCTION, PROCESSING, AND DISTRIBUTION OF FOOD
- MANUFACTURE OF SELECTED ELECTRONIC AND ELECTRIC EQUIPMENT, MACHINERY, AND VEHICLES
- DIGITAL SERVICE PROVIDERS
- RESEARCH
- NUCLEAR ENERGY INVESTMENTS
- PUBLIC ADMINISTRATION ENTITIES – AT THE LOCAL GOVERNMENT LEVEL

Size criterion

As a rule, the new regulations will apply to all medium-sized enterprises operating in the sectors listed in the annex to the Act, and in some cases, also to enterprises regardless of their size.

When calculating the size of an undertaking, in principle, linked undertakings (i.e., within a capital group) and partner undertakings (shareholding of at least 25%) should also be taken into account. However, the regulations provide for exceptions to this rule.

As a rule, the Polish regulations will apply to entities that have their registered office in Poland, as well as to those operating in Poland as a branch of a foreign undertaking or carrying out cross-border activities in Poland.

For certain categories of entities, the obligation to comply with the Polish regulations will depend on whether Poland is their main place of establishment, and the regulations set out how this criterion is to be verified. These rules apply, for example, to DNS service providers, domain name registrars, cloud computing service providers, content delivery network providers, managed service providers (MSPs), managed security service providers (MSSPs), online marketplace providers, online search engine providers, and social networking platform providers.

An essential or important entity must submit an application to be entered into the register within six months of the date on which it begins to meet the conditions for being classified as such an entity. This means that the fulfilment of the criteria must be monitored on an ongoing basis, as a delay may be treated as a breach of obligations.

⚠ **NOTE:** According to estimates by the Ministry of Digitalization, **more than 10,000 entities** will be subject to the listing obligation; according to some other estimates, this could be **up to 40,000 entities**.

Obligations

The obligations of essential and important entities are, to a large extent, identical.

The key obligation under the Act is **to implement an information security management system (ISMS)** within the information system used in processes that affect the provision of the entity's services. The Act sets out a number of requirements and elements that such a system should include, such as:

- carrying out systematic risk assessments of incidents and managing that risk,
- implementing technical and organizational measures that are appropriate and proportionate to the assessed risk, taking into account the latest state of knowledge and the entity's specific context,

NOTE: Technical and organizational measures should include, among others: risk assessment and information system security policies, human resources security, physical and environmental security, ensuring business continuity, monitoring the information system, assessing the effectiveness of the technical and organizational measures implemented, cybersecurity education for the entity's personnel, basic cyber hygiene principles, security and continuity of the supply chain for ICT products, ICT services, and ICT processes; asset management, and access control policies.

- collecting information on cyber threats and vulnerabilities relevant to incidents affecting the information system used to provide the service, and
- incident management, including the use of measures to prevent and mitigate the impact of incidents on the security of the information system.

NOTE: The legislator suggests the development of an incident management policy, the introduction of a device for reporting incidents within the entity, and the introduction of an incident-handling procedure.

Reporting of incidents

Incident-reporting obligations to the relevant sectoral CSIRT fall into a particular category. Essential and important entities which the new regulations apply to will be obliged, in principle, to:

- report an early warning of a significant incident as soon as possible and no later than 24 hours after the detection of the significant incident,
- report a significant incident within 72 hours with additional information about the incident, including a description of its impact on the services provided, a description of the causes of the incident, and information on the action taken,
- provide a progress report on the handling of the incident at the request of the sectoral CSIRT, and
- submit a final report on the handling of a significant incident no later than one month from the date it was reported.

What can the authority do?

Supervisory authorities will be entitled to take action in relation to supervised entities if they obtain a justified suspicion that an entity is not complying with the provisions of the Act. As part of their supervisory powers, the authority may, among others:

- carry out an inspection,
- require the entity to conduct an audit, and
- request the entity to provide documentation.

NOTE: If a breach of the Act is identified, the authority may issue binding recommendations or a decision specifying the measures to be taken to cease the infringement. Failure to comply with the obligations imposed by the authority's decision may result in further consequences, such as the suspension of a licence/concession.

What sanctions?

Failure to meet the new cybersecurity requirements may result in the imposition of administrative monetary penalties.

	ESSENTIAL ENTITY	IMPORTANT ENTITY
Minimum penalty	PLN 20,000	PLN 15,000
Maximum penalty	The equivalent of EUR 10,000,000 OR 2% of the revenue generated in the financial year preceding the imposition of the penalty (the upper threshold is determined by the higher penalty)	The equivalent of €7,000,000 OR 1.4% of the revenue achieved in the financial year preceding the imposition of the penalty (the higher amount determines the upper limit of the penalty)

NOTE : The competent authority will be able to impose a penalty of **up to PLN 100,000,000** if the essential entity or important entity, by violating the Act's provisions, causes a direct and serious cybersecurity threat to defense, state security, public safety and order or human life and health, or a threat to cause serious property damage or serious obstruction of services.

The Act provides that certain administrative monetary penalties may be imposed only after two years from the date the Act enters into force. This applies, among other things, to breaches such as a failure to be entered into the register or to update register data, a failure to implement the required security measures (including the ISMS), a failure to comply with incident reporting obligations, a lack of an audit, and a failure to comply with the authority's decisions/orders (including penalties for delay).

The manager of the essential entity or important entity may also be fined for failing to comply with the obligations set out in the act. The penalty may be imposed regardless of whether it is imposed on the essential entity or important entity.

	MANAGER OF AN ESSENTIAL OR IMPORTANT ENTITY	
Maximum penalty	300% of the salary received by the penalized person	A temporary ban on holding a managerial position or performing management functions until the deficiencies are remedied or the infringements cease.

Is that all? Where to start?

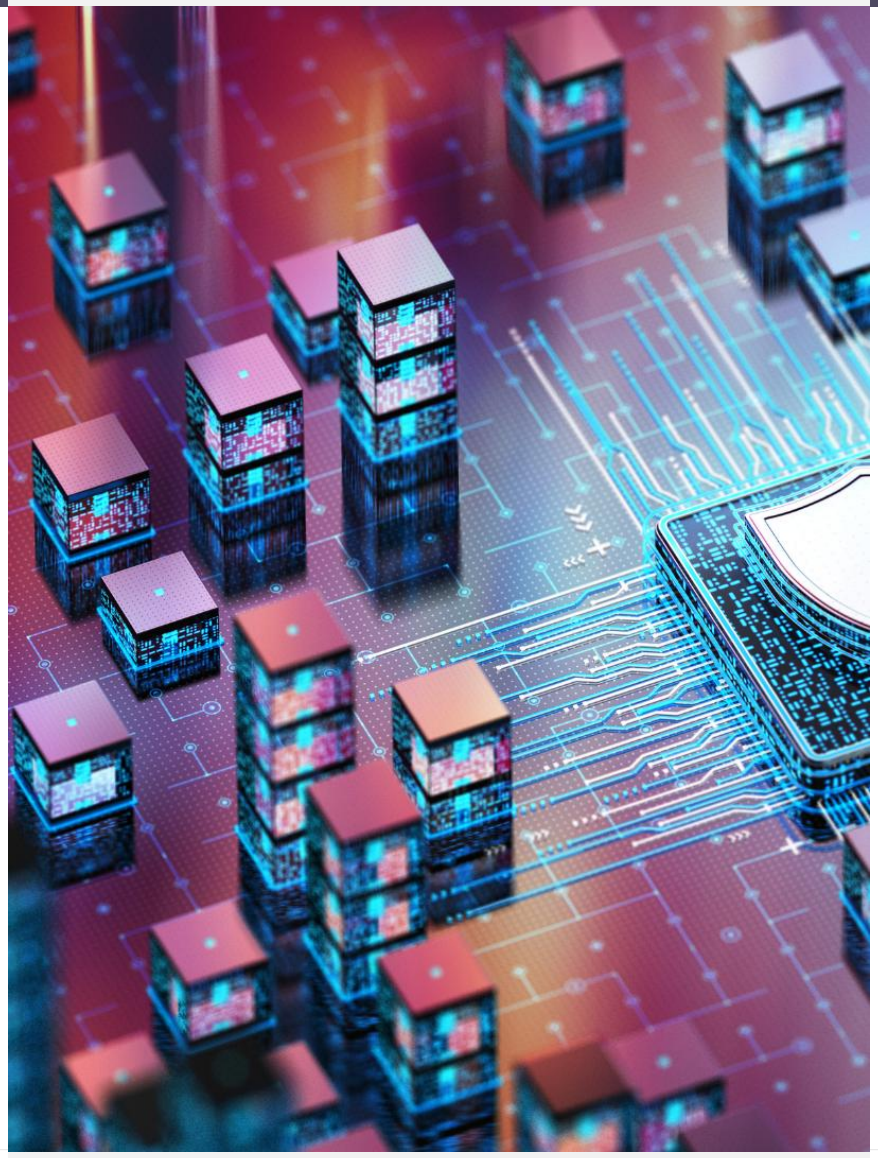
The new regulations will enter into force soon.

The short *vacatio legis* period and the deadline for implementing the new regulations mean that work on implementing the Act within an organization should begin as soon as it is promulgated; this is the last call to adapt to the new requirements. Some entities already foster a high level of cybersecurity awareness in their organisations and are prepared for the new rules. Others will only now begin to build that awareness.

Regardless of where your organisation currently stands, it is important to avoid rushing into ill-considered solutions. The measures adopted should be **appropriate** for the organization and proportionate to its capabilities and the actual risks it faces. **Compliance does not always have to mean purchasing expensive and advanced solutions**.

We believe that **the starting point is to make an honest self-identification**. We encourage you to start by using our QUESTIONNAIRE. The result of the survey can serve as the first clue to making a proper assessment of the reality your organization faces.

Go to the questionnaire



How can we help?

SK&S offers professional legal support in the process of self-identification, adaptation of the organization to upcoming legal requirements, and legal support in the incident handling process. We can also assist in the review and creation of internal procedures or contractual provisions with a particular focus on supply chain security.

We will be happy to answer additional questions and help you identify the areas that will be affected by the new regulations.

- Implementation advice
- Safeguarding the interests of entity managers
- Self-identification
- Support in handling and reporting incidents
- Policies and procedures
- DD support for transactions
- Contractual clauses (supply chain security)
- Tabletop exercise
- "Cyber" insurance
- Security of human resources

This material has been prepared to inform SK&S' clients of certain important changes in Polish law and does not constitute legal advice regarding the specific situation of any client and should not be treated by clients as advice. Should you have any questions related to the legal issues presented above and their possible impact on the business activities of a particular client in Poland, please contact us.

Contact us:

Michał Opala
Senior Counsel, attorney-at-law
✆ +48 602 402 617
✉ michal.opala@skslegal.pl

Mikołaj Sowiński
Partner, attorney-at-law
✉ mikolaj.sowinski@skslegal.pl

Tomasz Konopka
Partner, attorney-at-law
✆ +48 604 243 699
✉ tomasz.konopka@skslegal.pl

Warszawa
Jasna 26, 00-054 Warszawa
T +48 22 608 70 00
F +48 22 608 70 70
E office@skslegal.pl

Katowice
Korfantego 138a, 40-156 Katowice
T +48 32 731 59 86
F +48 32 731 59 90
E office.katowice@skslegal.pl

Poznań
Mickiewicza 35, 60-837 Poznań
T +48 61 856 04 20
F +48 61 856 05 67
E office.poznan@skslegal.pl

SOŁTYSIŃSKI KAWECKI SZLĘZAK