



Ministry of Digital Affairs  
Republic of Poland

---

# National Cybersecurity System 2.0

Amendment of the Act on NCS



# Essential Operators

- large entrepreneur with activities in key sectors;
- at least a medium-sized electronic communications company at least a small provider of managed cyber security services;
- regardless of size:
  - DNS service provider,
  - qualified trust service provider,
  - critical entity,
  - public entity,
  - entity identified as a critical entity by administrative decision,
  - top level domain name registry (TLD).

# Important Operators

- At least a medium-sized business operating in sectors 1 and 2;
- a non-qualified trust service provider which is a micro, small or medium-sized enterprise;
- an electronic communications undertaking which is a micro, small or medium-sized enterprise;
- an entity identified as a valid entity by an administrative decision.

# Registry of essential and important operators

## Listing obligation

- In 3 months

## clarification

- the range of public IP addresses used by the key entity or significant entity on a continuous basis
- Internet domains used by the key entity or valid entity on a permanent basis
- PESEL of the administrator of the entity's account in S46

# Other obligations




Provide the ability for a service user to report information about a cyber threat/vulnerability/incident

## Contact persons

- Micro, small entrepreneur shall appoint at least 1 person
- Other entities at least 2 persons



# Significant incidents reporting

-  Early warning – within 24 h
-  Report of the incident – within 72 h
-  Final incident report - within 1 month

Incidents will be reported via the S46 system to sectoral CSIRTs

The sectoral CSIRT shall report the incident to the national level CSIRT



# Penalties

## **Essential operator**

penalty not less than  
PLN 20 000 (~EUR 4 700)

not more than  
EUR 10 000 000  
or 2% of revenue

## **Important operator**

penalty of not less than  
PLN 15 000 (~EUR 3 500)

not more than  
EUR 7 000 000  
or 1.4% of revenue

# Date of entry into force

## Vacatio legis

- 1 month

## Adjustment period

- 6 months for essential/important operators to implement responsibilities
- OUKs to date report incidents within this period

## Registry of Essential/Important Operators

- Minister of Digital Affairs to launch list of key entities and valid entities within 1 month
- Registration schedule

Other EU files not to be  
forgotten...



# Council Recommendation on the EU Blueprint for cybersecurity crisis management

- Adopted during the Polish Presidency in the Council of EU
- Presents, in a clear, simple and accessible manner, the EU framework for cyber crisis management
- Enables relevant Union-actors to understand how to interact and make the best use of available mechanisms across the full crisis management lifecycle.
- Explains the use of available mechanisms like the Cybersecurity Emergency Mechanism, including the EU Cybersecurity Reserve, in preparing how to manage, respond to and recover from a crisis arising from a large-scale cybersecurity incident

# (Draft) Regulation to Prevent and Combat Child Sexual Abuse

- Aim of this legislation proposed in 2022 by the EC is to prevent child sexual abuse online through the implementation of a number of measures:
  - ✓ establishment of a harmonized legal framework at EU level;
  - ✓ detection and reporting of child sexual abuse material (CSAM) by digital platforms - a legal requirement within the European Union;
  - ✓ establishing a European Centre to prevent and counter child sexual Abuse.



Ministry of Digital Affairs  
Republic of Poland

---

# Thank You

Department of Cybersecurity  
[Sekretariat.DC@cyfra.gov.pl](mailto:Sekretariat.DC@cyfra.gov.pl)

