PEYTON legal

New Cybersecurity Act: personal liability for management and tough penalties starting in November!

On 4 August 2025, the new Cybersecurity Act ("**CSA**") was published in the Collection of Laws, transposing the requirements of the NIS2 Directive into Czech law. The new rules will take effect from 1 November 2025.

Once the CSA enters into force, cybersecurity obligations will newly apply to thousands of entities that have so far operated outside the regulatory scope. As with any new piece of legislation, the CSA introduces stricter requirements and consequently increased accountability for the management of affected companies.

We have therefore prepared a summary of the **key points** you need to be aware of in light of the upcoming legal changes.

Does the new cybersecurity regulation apply to you?

CSA applies if **your company (the provider):**

- provides a service essential to the continuity of critical activities or relevant to the security of the Czech Republic;
- operates in sectors such as energy, healthcare, transport, water management, digital infrastructure, managed ICT services, financial market infrastructure, banking, food industry, postal services, chemical industry; and
- qualifies as a medium-sized or large enterprise or is otherwise deemed essential for the provision of regulated services.

What obligations does the CSA introduce?

1/ Self-assessment and registration:

- Every provider falling within the scope of the CSA will be required to carry out a self-assessment to determine its classification under one of two supervisory categories – so-called "essential entities" (enhanced supervision), or "important entities" (lower supervision).
- Within three months of the CSA's entry into force, the provider must complete a formal registration with the Czech Cybersecurity Authority (CCA) via an electronic form.

Note: Incorrect or misleading information may also be subject to penalties – fines can reach up to CZK 250 million!

2/ Internal policies and process implementation

Providers will also be required to:

- adopt a cybersecurity policy;
- establish an asset inventory;
- revise supplier contracts in line with supply chain security requirements;
- implement a risk management process and conduct regular compliance audits in accordance with the new rules.

Additional obligations include training for management personnel and the implementation of measures for incident prevention.

Note – the CSA introduces personal liability for management!

The CSA newly empowers CCA to impose a temporary ban on serving as a member of a executive body. This may occur in cases of serious or repeated breaches of obligations, typically when company leadership fails to implement required security measures, disregards countermeasures imposed by CCA, or does not respond to cybersecurity incidents.

The ban lasts at least 6 months, takes effect immediately. The ban is published not only in the Commercial Register, but also on the CCA website.

This measure thus carries not only legal, but also significant reputational consequences.

We strongly recommend starting preparations immediately!

Key deadlines begin on the very first day of the entry into force as of 1 November 2025.

Maximum penalties under the CSA:

- up to CZK 250 million or 2% of global turnover (essential entities);
- up to CZK 175 million or 1.4% of global turnover (important entities).

Self-assessment, registration, and the implementation of internal processes require coordination, time, and expert support. Do not postpone preparation until the last minute – this will help you avoid unnecessary penalties and protect not only your management team but also your company's reputation.

Who can you contact?

If you're unsure whether the new regulation applies to you, or if you need support in ensuring compliance with the new rules, feel free to reach out to us.

Our team can assist you with the self-assessment process, the preparation of internal documentation, and the implementation of required measures in accordance with the CSA.

PEYTON legal Compliance team

Mgr. Jakub Málek
managing partner
malek@plegal.cz

Mgr. Martin Heinzel
partner
heinzel@plegal.cz

JUDr. Tereza Pechová
junior lawyer
pechova@plegal.cz