Deloitte.

Cybersecurity Act
Deloitte Cyber Regulatory Compliance

By transposing the **NIS2 Directive**, a new Cybersecurity Act No. 264/2025 Coll., was enacted in the Czech Republic, applicable from **1 November 2025**.

It significantly expands the scope of affected sectors, including the automotive industry, medical device and pharmaceutical product manufacturing, food processing and distribution, waste management, and others. There are **two obligation regimes**, allowing the scope of regulatory requirements to be adapted according to the size and strategic importance of the organization.

Lower Regime applies to organizations that, while being regulated, would have a **lower impact** in the event of a disruption.

Higher Regime applies to entities whose activities are considered **critical**., e.g., from the perspective of public services.

Both regimes establish the duty to **implement security measures**, **report cybersecurity incidents**, and comply with **basic cybersecurity rules**, while differing in the extent of obligations and depth of implementation.

WHO DOES THE CYBERSECURITY ACT APPLY TO?

Deloitte.

In line with the NIS2 Directive, the Czech Cybersecurity Act defines regulated services, including the following:

- PUBLIC ADMINISTRATION
- ENERGY
- MANUFACTURING
- FOODS
- CHEMICALS
- WATER SUPPLY
- WASTE MANAGEMENT
- TRANSPORT
- DIGITAL INFRASTRUCTURE
- FINANCE
- HEALTH
- RESEARCH
- POSTAL SERVICES
- SPACE
- DEFENSE

Many regulated service providers must conduct a **self-assessment** to determine whether they fall under the Cybersecurity Act, considering not only their business sectors but also:

Strategic Importance

› Strategic service providers, whose disruption could have a **serious impact on the security** of the Czech Republic or public order.

Enterprise Size & Turnover

› At least **50 employees** and a turnover of at least **EUR 10 million**.

This criterion does not apply, for example, to **trusted service providers**, **DNS service providers**, or **TLD managers**.

Competent authority: The competent regulator is **NÚKIB**.

SELECTED REQUIREMENTS

Affected entities are obliged to:

› **Notify NÚKIB** no later than **60 days** from the date the criteria for registration of a regulated service are met.
› Implement **security measures** within 1 year from the date of delivery of the decision on the registration of a regulated service.
› Conduct **self-assessment** and designate the role of a Cybersecurity Manager.
› Conclude **contracts with a third-party suppliers** reflecting the legal requirements.

HOW CAN DELOITTE HELP?

Deloitte.

Through cooperation between Deloitte teams, we will provide you with services that ensure full compliance with the Cybersecurity Act and related regulations, such as GDPR and the EU AI Act, both from a legal and a technical perspective.

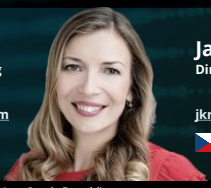
We provide the following services and more:

- **Applicability Assessment**
- **Legal Advisory**
- **Gap Analysis**
- **Risk Analysis & Evaluation of Existing Processes**
- **Remediation Measure Identification**
- **Regulatory Requirement Implementation Support**
- **Training & Educational Program Design**
- **Internal Documentation Review & Update**
- **Supply Chain Evaluation & Revision**

The very first step to compliance lies in a **comprehensive analysis**, displaying areas of improvement. We use our **own proven tools** in such analyses. Start by self-assessing your maturity using our **NIS2 Maturity Self-Assessment Tool**.

CONTACT US

Jakub Höll
Director, Consulting
CZ & SK Cyber Lead
jholl@deloittece.com



Jaroslava Kračúnová
Director, Legal
jkracunova@deloittece.com

Pavol Szabó
Senior Managing Associate, Legal
pszabo@deloittece.com