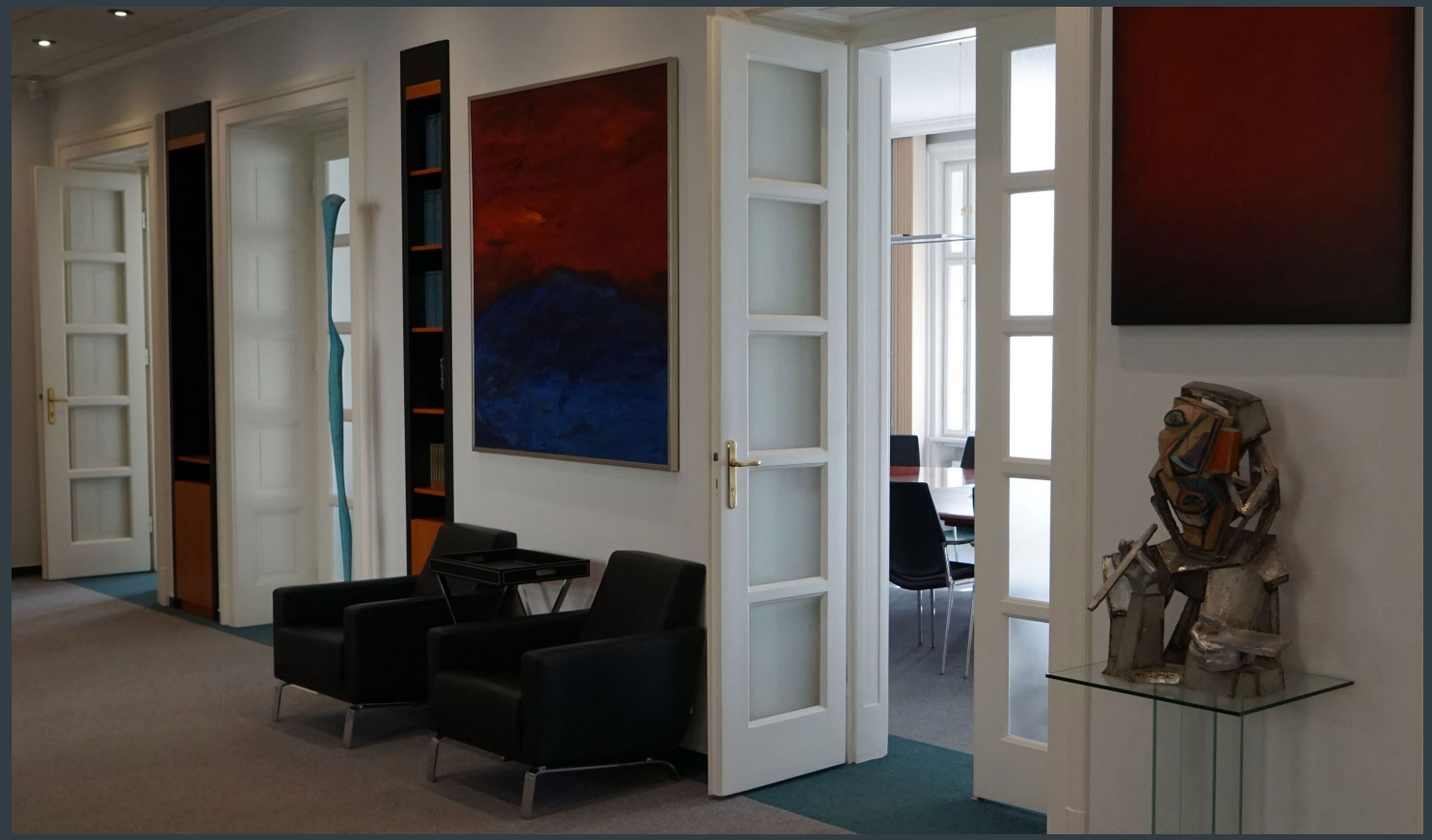
SZECSKAY



THE NIS2 DIRECTIVE AND THE HUNGARIAN EXPERIENCE

THE NIS2 DIRECTIVE

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union

Needed to be implemented by 17 October 2024

Minimum harmonisation: Member States may adopt/maintain provisions which ensure a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law

SZECSKAY

THE NIS2 DIRECTIVE

Member States must

- adopt a national cybersecurity strategy
- designate one or more supervisory authorities
- designate computer security incident response teams (CSIRTs)
- ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems
- ensure that essential and important entities notify, without undue delay, its CSIRT

SZECSKAY

THE HUNGARIAN IMPLEMENTATION

Act no. LXIX of 2024 on the Cybersecurity of Hungary

Governmental Decree 418/2024 on the Execution of the Act

Decree by the Chef of the PM’s Cabinet on the requirements of the classification of information systems and security measures (the Decree comprises more than 120 pages: 6 pages contain the classification criteria and 116 pages contain a list of security measures required)

Decrees by the supervisory authority (e.g. registration of entities, registration of auditors, annual supervision fees, fines, audit methodology)

SCOPE OF THE ACT

To be examined if the entity falls under the Act

To decide this in case of a private entity, one needs to take into account:

- activities of the entity (Annexes 2 and 3 of the Act: significantly risky and risky sectors),
- number of employees and revenues for the last two years on a group level

SZECSKAY

MAIN OBLIGATIONS UNDER THE ACT

Risk management framework

The head of the organisation (HoO) is required to establish and operate a **risk management framework** for the protection of the electronic information systems (EIS): e.g.

- defining the roles, responsibilities, tasks and the necessary competences relating to the security of the EIS of the organisation,

- designating or concluding a contract with the person responsible for the security of the EIS (PR),

- performing impact analysis and risk management activities,

- making sure that the security measures are duly enforced and periodically evaluated,

- issuing information security policy and reviewing it every two years.

Designation of a PR

The HoO is required to **designate a PR within the organisation or to conclude an agreement with a PR** outside the organisation in order to perform the tasks related to the protection of the EIS, to operate the risk management framework, to report cybersecurity incidents and to liaise with the cybersecurity incident management centre.

MAIN OBLIGATIONS UNDER THE ACT

Requirements for the PR:

- full legal capacity,
- clean criminal record,
- properly qualified with the necessary knowledge and experience.

The HoO must ensure that the PR

- attends trainings,
- participates in the preparation of all decisions concerning the security of EIS,
- has at his/her disposal the necessary conditions, privileges, information, human and material resources to ensure the security of the EIS
- has access to all systems, data and information necessary for the performance of the tasks for which he/she is responsible.

MAIN OBLIGATIONS UNDER THE ACT

PR bound by confidentiality obligations with regard to the data and information that he/she becomes aware of in the course of his/her duties

SZECSKAY

MAIN OBLIGATIONS UNDER THE ACT

Classification of EIS

Within the framework of the risk management activity, the HoO is required to **classify each EIS into a security class** (basic, significant, high)

Result of the security classification to be recorded by the organisation in the register of EIS or other internal by-laws

Classification to be performed prior to contracting with the auditor

The requirements for security classification and the specific security measures applicable to each security classification are provided in specific ministerial decree

Security classification **to be reviewed in a documented manner at least every two years** or, on an ongoing basis, in the event of a statutory change affecting the security of the EIS

MAIN OBLIGATIONS UNDER THE ACT

Cybersecurity audit

Private organisations falling within the scope of the Act are required to **conduct a cybersecurity audit every two years**, or if so ordered by the supervisory authority

Contract with the auditor to be concluded by 31 August 2025, the first audit to be conducted by 30 June 2026

Audit can be conducted by

a) an auditor registered with the supervisory authority and licensed to conduct audits for “basic", "significant" or "high" security class systems in respect of “basic” EIS,

b) an auditor registered with the supervisory authority and licensed to conduct audits for "significant" or "high" security class systems in respect of “significant” EIS, and

c) an auditor registered with the supervisory authority and licensed to conduct audits for "high" security class systems in respect of “high” EIS.

Auditor to verify the security classification of the EIS and the adequacy of the security measures according to the security classification and to send the result of the audit to the supervisory authority and the organisation

MAIN OBLIGATIONS UNDER THE ACT

Payment of annual supervisory fee

In general, the amount of the fee is set at

(i) 0.00015% of the annual net turnover as per the closed and submitted annual financials for the year preceding the reference year, if the annual net turnover of the organisation in the year preceding the reference year is less than HUF 20 billion (about EUR 50 million),

(ii) 0.0015% of the annual net turnover as per the closed and submitted annual financials for the year preceding the reference year, but not more than HUF 10 million, if the organisation's annual net turnover for the year preceding the reference year is equal to or exceeds HUF 20 billion (about EUR 50 million).

The fee may not exceed HUF 10 million (about EUR 25,000) (and, in case of companies under joint control belonging to the same group, HUF 50 million (about EUR 125,000)).

MAIN OBLIGATIONS UNDER THE ACT

Payment of audit fee (decree about the maximum amount)

Fee depends on (i) the net turnover for previous year, (ii) the number of EIS and (iii) the classification of the EIS

Maximum fee between HUF 1,575,000 (about EUR 3,940) and HUF 140,000,000 (about EUR 350,000)

MAIN OBLIGATIONS UNDER THE ACT

Registration with the supervisory authority

A private organisation falling within the scope of the Act must, within 30 days after commencing its operations or coming within the scope of the Act, **notify certain data to authority** for the purposes of registration

Notification to be made electronically

SZECSKAY

MAIN OBLIGATIONS UNDER THE ACT

Use of third party's services

If the entity engages a contractor to create, operate, audit, maintain or repair EIS or to manage cybersecurity incidents or to perform data processing activities related to the entity's EIS, the HoO is obliged to **ensure that the cybersecurity requirements in connection with the activities performed by the contractor in relation to the EIS are fulfilled as a contractual obligation**.

MAIN OBLIGATIONS UNDER THE ACT

Appointment of representative

An organisation operating an EIS subject to the Act and not registered in Hungary is required to **appoint in writing a representative based in Hungary**, who will be responsible for the implementation of the provisions of the Act. The designation of the representative does not affect the liability of the organisation or the head of the organisation.

MAIN OBLIGATIONS UNDER THE ACT

Management of cybersecurity incidents

Entities to **report to the national cybersecurity incident management center threats, near-cybersecurity incidents and cybersecurity incidents**, including operational cybersecurity incidents, that occur in their EIS or come to their knowledge, which cause serious disruption or material damage to the operation of the organisation or the provision of services rendered by it, or cause significant material or non-material damage to other natural or legal persons.

Furthermore, the organisation to **take appropriate measures to address the cybersecurity incident**.

If the management of the cybersecurity incident exceeds the capabilities of the entity, the entity may contact the sectoral cybersecurity incident management centre or the national cybersecurity incident management centre to manage the cybersecurity incident concerned.

SANCTIONS

Sanctions

If the organisation fails to comply with the security requirements and related procedural rules, fails to remedy the security deficiencies, fails to take the necessary measures for compliance or does not cease the activity, the authority, amongst others,

a) warns the entity to comply with the legal security requirements and related procedures, and requires it to take the necessary measures to comply with the requirements, by setting an appropriate deadline,

b) may order the cessation of the infringement, and

c) may appoint an information security supervisor at the expense of the organisation.

SANCTIONS

Fine

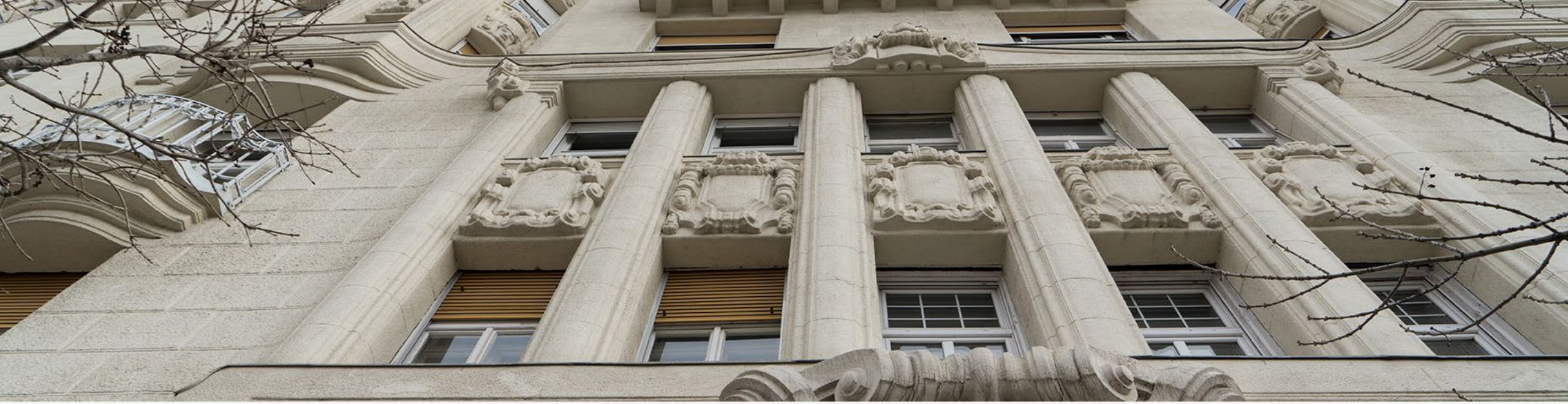
If, despite the application of the measures, the entity concerned fails to comply with the security requirements, fails to remedy the security deficiencies, fails to take the necessary measures to comply, the authority may impose a fine.

Amount of fine depends on the type of entity and the type of violation

For example, in the event of failure to establish/operate a risk management framework, the maximum amount can go up to

- an amount in HUF equal to EUR 10 million or, if it is higher, an amount equal to 2% of the total amount of the organisation's global annual turnover in the preceding financial year, in case of an essential entity,

- an amount in HUF equal to EUR 7 million or, if it is higher, an amount equal to 1.4% of the total amount of the organisation's global annual turnover in the preceding financial year, in case of an important entity.



THANK YOU FOR YOUR ATTENTION!

SZECSKAY

info@szecskay.com
+36 1 472 3000

www.szecskay.com