Hungary

Your local contact

Dr. Csilla Dékány
Attorney-at-Law, Law Firm Partner, PwC Legal Hungary
+36 30 528 1907
csilla.dekany@pwc.com

Dr. András Csenterics LL.M.
Attorney-at-Law, Law Firm Partner, PwC Legal Hungary
+36 30 866 1797
andras.csenterics@pwc.com

Status	Implemented
Name of National Law	Act LXIX of 2024 on the cybersecurity of Hungary (the Act)
Entered into force	1st January 2025
Link to current draft or equivalent	https://njt.hu/jogszabaly/2024-69-00-00 ; https://net.jogtar.hu/jogszabaly?docid=a2400069.tv; English translation is currently not available.
Scope (deviating from NIS-2-Directive)	(Additional) categories of entities in scope: Entities identified as essential or important by the national cybersecurity authority / national defense cybersecurity authority, certain entities belonging to the administrative sector, entities engaged in national defense interests.
Registration	All entities within scope must register with their respective authority within 30 days of their commencement of operation or from the date upon which they fell under the scope of the Act.
Information Security Standards referenced	The Act does not specify any standards; however, the Act states that for an entity to ensure compliance with specific obligations, ICT products, services or processes that have been certified pursuant to Hungarian or European cybersecurity certification schemes could be eligible. The regulator reserves the right to enact further decrees making specific entities obliged to utilize ICT products, services, processes that have been certified pursuant to Hungarian or European cybersecurity certification schemes to comply with the Act.
Incident reporting	All entities within scope are required to report cybersecurity events to the National Cybersecurity Center of Hungary.
Authority / CSIRT	Supervisory Authority of Controlled Activities, SZTFH (supervisory authority), Special Service for National Security or the Minister of Defence depending on the type of entity, National Cybersecurity Center of Hungary (CSIRT).
Fines (deviating from NIS-2-Directive)	Maximum fines as in NIS-2. Government Decree 418/2024. specifies the minimum and maximum of fines that could be imposed for each type of the violation. **In case of entities operating in sectors of high criticality, or other critical sectors**: • Failure to register after the deadline: From HUF 50.000 (~EUR 125) up to HUF 15.000.000 (~EUR 37.500). • Failure to register at all: From HUF 1.000.000 (~EUR 2.500) up to HUF 150.000.000 (~EUR 375.000) • Failure to pay supervisory fee: From HUF 500.000 (~EUR 1.250) up to 10 times the supervisory fee imposed (HUF 500.000.000 ~ EUR 1.250.000) • Failure to create and operate a risk management framework: From HUF 1.000.000 (~EUR 2.500) up to NIS-2 maximum • Failure to conduct cybersecurity audit in time: From HUF 1.000.000 (~EUR 2.500) up to HUF 50.000.000 (~EUR 125.000)

Hungary

Your local contact

Dr. Csilla Dékány
Attorney-at-Law, Law Firm Partner, PwC Legal Hungary
+36 30 528 1907
csilla.dekany@pwc.com

Dr. András Csenterics LL.M.
Attorney-at-Law, Law Firm Partner, PwC Legal Hungary
+36 30 866 1797
andras.csenterics@pwc.com

Fines (deviating from NIS-2-Directive)	**Fines for the head of the organization**: In case of non-compliance of obligations set in the Act being the responsibility of the head of the organization, the supervisory authority might, in case of recurring infringements, the supervisory authority shall impose a fine up to HUF 15.000.000 (~EUR 37.500) on the head of the organization. • Deadline for fines imposed: The fine must be paid within 8 days of the decision of the cybersecurity authority becoming final and binding. • Recurring non-compliance: The fine may be imposed again under the same circumstances after two months have passed since the notification of the final decision imposing the fine.
Worth mentioning	• For certain entity types only the utilization of ICT products, ICT services or ICT processes certified by European or national cybersecurity certification systems might be suitable for demonstrating actual compliance. • Classification of information security systems into security levels (basic, significant, high) shall take place according to the rules set forth in MK Decree 7/2024. Such classification is a necessary pre-requisite of fulfilling the obligations set forth in the Act. • The first cybersecurity supervision fees for the years of 2024 and 2025 have been imposed by the SZTFH. These should be paid till **31 July 2025**. • Entering into contract with the cybersecurity auditors shall be concluded **by 31 August 2025**. • The first cybersecurity audit shall be conducted till **30 June 2026**. • If contributors are engaged for the creation, operation, auditing, maintenance or repair of electronic information systems, the management of cybersecurity incidents, or the performance of data processing activities related to electronic information systems of an entity within scope, such entity shall ensure that the cybersecurity requirements regarding the systems concerned are reflected through adequate contractual obligations in accordance with the provisions of the Act and are thereby binding on the given contributor.