Lithuania

Your local contact

Rokas Bukauskas
Partner, PwC Legal Lithuania
+370 657 99250
rokas.bukauskas@pwc.com

Status	Implemented
Name of National Law	Republic of Lithuania Law on Cyber Security; Resolution of the Government
Entered into force	18th October 2024; 12th November 2024
Link to current draft or equivalent	https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr
Link to the current resolution	https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
Scope (deviating from NIS-2-Directive)	(Additional) categories of entities in scope: Essential and important entities which are also medium-sized and large enterprises, DNS-service providers. Additional national criteria have been established that are not provided for in the NIS-2-Directive and according to which entities would be classified as essential or important entities, e.g. identification criteria related to the provision of third-party services to the public administration sector and essential entities, identification criteria related to entities carrying out essential research and experimental development activities in the research sector, etc. Jurisdiction was extended to DNS service providers and other similar persons whose head office is in the Republic of Lithuania, if these entities are registered or established in the Republic of Lithuania, which is not included in the NIS-2-Directive. When determining functions related to cooperation in the field of cybersecurity, in addition to cooperation with the EU, NATO and other states, as well as EU, NATO institutions and international organizations, are involved.
Registration	Essential and important entities. Registration is mandatory via the cybersecurity information system (the register is fully completed from 17 April 2025), administered by the National Cybersecurity Center.
Information Security Standards referenced	**LST EN ISO/IEC 27002:2023** (same as **ISO/IEC 27002:2022**. Information security, cybersecurity and privacy protection - Information security controls).
Incident reporting	Very important entities and important entities must report significant security incidents to the National Cybersecurity Center.
Authority / CSIRT	National Cybersecurity Center
Fines (deviating from NIS-2-Directive)	• Follows NIS-2-Directive. Fines depend on entity (essential of important and legal person or budgetary institution) and danger of infringement (dangerous, medium danger, low danger). Provision in the Article 34(6) of the Directive about periodic fines was not implemented. • Managers or other responsible persons of legal entities are subject to a fine of EUR 250 to EUR 3.000 for violating the requirements set out in the Law on Cybersecurity, and a repeated offense incurs a fine of EUR 2.000 to EUR 6.000.
Worth mentioning	There is provision stating that Cybersecurity entities shall conduct a cybersecurity audit at least once every 3 years, according to the cybersecurity audit methodology approved by the National Cyber Security Centre.