National Cyber Security Law

May 2024

The National Cyber Security Law aims to enhance cybersecurity in Latvia and the European Union by establishing a National Cyber Security Centre and transposing the new EU Directive NIS2 into the Latvian legal system. These changes will introduce new cybersecurity requirements for additional sectors, as well as for other sectors if the service provider meets the criteria of being an important and essential service provider. The new law mandates that every entity appoint a cybersecurity manager and introduces several other significant changes.

National Cyber Security Centre

The National Cyber Security Centre will be tasked with monitoring essential and critical service providers, coordinating national cybersecurity policy, developing a national cybersecurity strategy, and overseeing the implementation of cybersecurity requirements. The functions of the National Cyber Security Centre will be performed by the Ministry of Defence in cooperation with CERT.LV, thus combining the development and coordination of national cyber security policy, which is the responsibility of the Ministry of Defence, and incident prevention, which is the responsibility of CERT.LV.

Who will be targeted by the new law?

The forthcoming legislation will broaden the scope of sectors subject to cybersecurity regulations. Specifically, digital services, postal services, courier services, chemicals, food production, wholesale and retail trade, waste management, industrial production, and all Latvian universities will fall under the purview of the expanded cybersecurity requirements. The law will also apply to providers of essential and critical services. In one case, the law itself will define which entities, regardless of size, will be considered essential and critical service providers. In the second case, the law will include criteria for an entity to be considered an essential and critical service provider.

Important and essential service providers

Articles 18 and 19 of the draft law list entities designated as important and essential service providers. This includes large economic operators in specific sectors, electronic communications operators, and others as important service providers. Medium economic operators, operators in certain sectors, operators of educational information systems, and others are classified as essential service providers. Companies and organizations must self-assess their status based on these articles and submit notifications to the National Cyber Security Centre and the Office for the Protection of the Constitution by 1 April 2025.

Sanctions

The proposed legislation grants authority to the National Cyber Security Centre and the Office for the Protection of the Constitution to enforce legal obligations, including the imposition of fines for non-compliance. Essential service providers may face penalties of up to 10 million euro or 2% of their total annual worldwide turnover, while critical service providers may face penalties of up to 7 million euro or 1.4% of their total annual worldwide turnover. If obligations are not met, fines may be imposed.