COBALT

Summary of Latvia's New National Cyber Security Law

On 1 September 2024, the National Cyber Security Law came into force. This law, adopted by Parliament on 20 June 2024, replaced the Law on the Security of Information Technologies. The new legislation aims to bolster and enhance cybersecurity in Latvia, as well as implement the revised 2022 EU Network and Information Security Directive or "NIS2", which aims to establish a high common level of cybersecurity across the European Union (EU). With the implementation of the NIS2 directive in Latvia, cybersecurity requirements will be significantly increased and the range of industries required to comply with cybersecurity regulations will broaden. According to the Ministry of Defence's estimates, the new law will apply to over 2,000 entities. Consequently, with this expanded scope, a high common level of cybersecurity will be ensured across different sectors in Latvia, including both public and private sectors. Entities subject to the law will need to register by 1 April 2025.

Expanded Scope of Subjects

The National Cyber Security Law will apply to both essential and important service providers, as well as to the information and communication technology (ICT) critical infrastructure. Therefore, the new law will replace the categories of "basic service providers" and "digital service providers" as outlined in the Information Technology Security Law, with "**essential service providers**" and "**important service providers**". Articles 20 and 21 of the new law set out the criteria by which public and private sector organisations are classified into one of these groups. The criteria for company inclusion are based on both the industry in which they operate and the size and financial turnover of the company. As before, the institutions and companies included in the ICT critical infrastructure list will be approved by the Cabinet of Ministers.

Essential Service Providers

- Registry of top-level domain names
- Domain name system service provider
- Electronic communications network provider
- Qualified trust service provider
- Institutions of direct administration, state entities and private law legal entity performing a task delegated by the state administration (except state security institutions)
- Derived public entities
- Public electronic mass media
- An institution or economic operator whose disruption could have a significant impact on public safety, public security, public health or could create a significant systemic risk, especially in sectors where such disruption may have cross-border effects
- A large-sized enterprise, the only provider of a specific service in Latvia, or an intermediate administrative institution that operates in:
  - **energy sector** (energy supply, oil supply, hydrogen supply)
  - **transport sector** (aeronautical services, aircraft operators, operators of airfields or other civil aviation facilities and equipment, railway carriers, railway infrastructure managers, shipping companies, port authorities, merchants who carry out commercial activities in the port area, merchants who manage state highways or carry out state road infrastructure maintenance works, operators of intelligent transport systems)
  - **medical and pharmaceutical sector** (medical institutions, EU reference laboratory, traders carrying out research and development activities in relation to medicines, producing medicines and active substances, manufacturers of critical medical devices)
  - **water supply sector** (drinking water supplier or distributor, water management service provider)
  - **telecommunications and ICT sector** (internet flow exchange point services, cloud computing services, data centre services, content delivery network services, information and communication technology management or cyber security service providers, online search engine service providers, social media platform service providers)
  - **financial services sector** (credit institution, central business partner or trading place within the meaning of the Financial Instrument Market Law)
  - **space industry**

Important Service Providers

- A medium or large-sized enterprises, the only provider of a specific service in Latvia, or an intermediate administrative institution that operates in:
  - **postal and courier sector**
  - **waste management sector**
  - **chemical** manufacturing, production, and wholesale distribution
  - **food** production processing and wholesale distribution
  - **manufacturing** (manufacturing of medical devices, computers, electronic and optical equipment, equipment not elsewhere classified, mechanisms and machinery, vehicles, trailers and semi-trailers, other transport equipment)
  - **digital services** (providers of online marketplaces, providers of online search engines, providers of social networking services platforms)
  - **security services**
  - **scientific institution**
- The maintainer of the educational information system, which performs electronic processing of the data of the students of educational institutions accredited in Latvia
- A trust service provider that is not a qualified trust service provider
- A medium-sized enterprises who operates in:
  - **energy sector** (energy supply, oil supply, hydrogen supply)
  - **transport sector** (aeronautical services, aircraft operators, operators of airfields or other civil aviation facilities and equipment, railway carriers, railway infrastructure managers, shipping companies, port authorities, merchants who carry out commercial activities in the port area, merchants who manage state highways or carry out state road infrastructure maintenance works, operators of intelligent transport systems)
  - **medical and pharmaceutical sector** (medical institutions, EU reference laboratory, traders carrying out research and development activities in relation to medicines, producing medicines and active substances, manufacturers of critical medical devices)
  - **water supply sector** (drinking water supplier or distributor, water management service provider)
  - **telecommunications and ICT sector** (internet flow exchange point services, cloud computing services, data centre services, content delivery network services, information and communication technology management or cyber security service providers, online search engine service providers, social media platform service providers)
  - **financial services sector** (credit institution, central business partner or trading place within the meaning of the Financial Instruments Market Law)
  - **space industry**

Criteria for Medium and Large Enterprises

Medium−sized enterprise — a legal or natural person or an association of such persons, which carries out economic activity in the Republic of Latvia and meets all the following criteria:

1) enterprise employs up to 249 employees;
2) the total net turnover of the enterprise of the last financial year is at least 10 million euros, but does not exceed 50 million euros, or the total amount of the annual balance sheet is at least 10 million euros, but does not exceed 43 million euros.

Large−sized enterprise — a legal or natural person or an association of such persons, which carries out economic activity in the Republic of Latvia and meets at least one of the following criteria:

1) enterprise employs at least 250 employees;
2) the total net turnover of the enterprise in the last financial year exceeds 50 million euros and the total amount of the annual balance sheet exceeds 43 million euros.

The Main Requirements of Subjects

Requirement to register until 01.04.2025	Companies and institutions will have to self-assess their compliance with the law. In case of compliance, the essential or important service provider status will have to be notified electronically to the National Cyber Security Centre by **1 April 2025.**
Requirement to appoint the responsible person by 01.10.2025	Each subject will be obliged to appoint a cyber security manager and notify the competent authorities about it by **1 October 2025**. The appointment of such a manager will contribute to the effective management and security of the ICT infrastructure. The requirements of the cyber security manager will be determined in the upcoming Cabinet of Ministers Regulations on The Minimum Cyber Security Requirements, which are currently still under development. The new regulations are planned to be adopted by 17 October 2024. A cyber security manager is expected to meet minimum qualifications and security requirements.
Requirement to submit a self-assessment report by 01.10.2025	By **1 October 2025**, subjects will be required to submit a self-assessment report. This report must indicate whether the legal entity complies with the statutory requirements and explain any non-compliance, if applicable. The self-assessment report form will be available under the new Cabinet of Ministers regulations. The report must be submitted once every three years unless the subject belongs to security class A, who are required to submit the report annually. It is important to note that in the event of non-compliance, the subject may be required to conduct an external audit, the cost of which will be borne by the subject itself.
Requirement to comply with minimum cyber security requirements	The law mandates the adoption of suitable and proportionate technical and organisational measures to manage cyber risks and prevent or minimise the transmission of cyber incidents to the entity's service recipients and other services. Therefore, subjects will be required to organise cyber security management processes, maintain cyber hygiene, assess confidentiality, integrity, and disruption risks, and develop risk mitigation measures and a cyber risk management and ICT business continuity plan. The forthcoming regulations from the Council of Ministers will determine the requirements for the type of entities and their respective risk categories. These new Cabinet of Ministers regulations will replace the existing Cabinet of Ministers Regulations of 28 July 2015 No. 442 "Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements", which will expire on 18 October this year.
Duty to report cyber security incidents	In the event of cyber security incidents, the procedure for reporting to the competent authorities will be established. Until now, the reporting requirements were contained in several regulatory acts, which will now be consolidated into the National Cyber Security Law. Upon detection of a cyber incident, **the subject must immediately take all necessary actions to prevent a cyber incident, as well as immediately inform the competent cyber incident prevention institution** about the cyber incident and comply with its instructions regarding actions in the event of a cyber incident. A major cyber incident will necessitate an early warning to be submitted immediately, but no later than 24 hours, and initial reporting of a major cyber incident will be required within 72 hours (within 24 hours for a reliability service provider). However, the reporting of any detected incident, near-miss cyber incident or cyber threat is encouraged, as competent authorities can assist in preventing them and involve operational authorities as needed. Voluntary reporting of a near-miss cyber incident, or cyber threat will not impose additional obligations on the subject.

In Case of Non-Compliance – Significant Fines

The law stipulates the application of fines and enforcement rules in the event of significant non-compliance. Competent authorities will have the power to impose penalties:

- For essential service providers, **up to 10 million euros**, but if the total amount of net turnover of the previous financial year exceeds 500 million euros, **up to 2% of the net turnover**.
- For providers of important services, **up to 7 million euros**, but if the total net turnover of the previous financial year exceeds 500 million euros, **up to 1.4% of the net turnover**.
- **Up to 10 million euros** for the owner or legal holder of ICT critical infrastructure, but if the total net turnover of the previous financial year exceeds 500 million euros, **up to 2% of the net turnover.**

The Cabinet of Ministers will establish the procedure for determining the net turnover of the financial year, from which the fine is calculated, and the criteria for determining the fine amount.

For more details or in case of questions please contact COBALT specialists:

Indriķis Liepa
Partner
indrikis.liepa@cobalt.legal

Agnese Gerharde
Senior Associate
agnese.gerharde@cobalt.legal