RÖDL

We pave the way.
Worldwide.

roedl.ee

NIS2 directive

February 2026

The rapid development of technology makes cyber security an increasingly important field. In recent years, both the number of cyber-attacks and their complexity have increased in the European Union. Therefore, it is particularly important to achieve a higher level of cyber security throughout the European Union.

In this newsletter you can find:

- Persons who fall under the scope of the Cyber Security Act
- Obligations of the new subject of the Cyber Security Act
- What happens when the law is not enforced

Dear reader,

We would like to inform you that on December 10, 2025, the Riigikogu has adopted a law to transpose the 2nd Cyber Security Directive (NIS2) into Estonian law and amend the Cyber Security Act. The changes have entered into force on January 1, 2026.
We have previously issued a newsletter[1] in which we provided an overview of the draft act for the transposition of the NIS2 directive. By now, the Estonian Cyber Security Act has been brought into conformity with the NIS2 directive. Since the Cyber Security Act, that had been in force before 01.01.2026, mostly regulated the cyber security requirements of the NIS2 directive, there was no necessity to make significant changes in Estonian law in order to transpose the directive.
Below we will examine to what extent the NIS2 directive has been transposed into Estonian law, who belongs in the scope of application of the law and what obligations come with being a subject of the law.

Persons who fall under the scope of the Cyber Security Act

The main change made in the law is the addition of the list of persons within the scope of application of the Cyber Security Act with the subjects prescribed by the NIS2 Directive, which has led to the expansion of the existing requirements to new subjects (primarily in the private sector). Thus, it is possible that companies that were not covered by the Cyber Security Act based on the NIS1 Directive may now fall within the scope of the Cyber Security Act with the adoption of the NIS2 Directive. According to the draft act, after the adoption of the directive approximately 3,000 subjects will be added to the list of subjects within the scope of application of the law.
The requirements of the Cyber Security Act apply to critical ("vital" in the directive) and important service providers. It should be noted that all vital service providers are automatically vital entities, but not all vital entities are automatically vital service providers. In order to avoid terminological confusion, instead of the term used in the directive "vital entity", the term "critical entity" was introduced in the Cyber Security Act.
Some of the persons named in the Cyber Security Act fall within the scope of application of the law, regardless of their size and turnover. The corresponding entities are listed in subsections 2 and 4 of § 3 of the Cyber Security Act. However, companies not named in said provisions fall within the scope of application of the Cyber Security Act only if they meet certain thresholds for the number of employees and turnover or balance sheet volume and operate in the field listed in the law (subsections 3 and 5 of § 3 of the Cyber Security Act).

Obligations of the new subject of the Cyber Security Act

Since the aim of the directive is to ensure a clear overview of the entities within the scope of application, each Member State is obliged to draw up a list of critical and important entities and entities providing domain name registration services.
Entities that fall within the scope of application of the law as of January 1, 2026 must submit information about the company, the sector and sub-sector of service provision, and the list of countries where it provides services to the supervisory authority, i.e. The Information System Authority, within three months from the date of compliance with the characteristics of a service provider.
Subjects of the new Cyber Security Act must start ensuring cyber security, i.e. implementing security measures within three years of becoming a subject of the Cyber Security Act, i.e. January 1, 2026. Thus, subjects of the new Cyber Security Act have until December 31, 2029, to bring their activities into conformity with the requirements of the Cyber Security Act and start complying with them. Please note that, while according to the previous requirements security measures generally in the private sector were to be applied to a specific service (activity),

[1] Transposition of the NIS2 Directive into national law – what is the current state in Estonia? Available: https://www.roedl.ee/en/, heading ”Publications”

the NIS2 directive stipulates that hereafter these measures must be applied to the entire organization of the subject.
In case of a cyber incident of significant impact, the units are obliged to immediately notify the supervisory authority (The Information System Authority), who is responsible for the resolution of the cyber incident.

What happens when the law is not enforced

The Information System Authority (RIA) carries out national and administrative supervision over the fulfillment of the requirements set forth in the Cyber Security Act.
RIA, as a supervisory authority, has the right to limit the use of the system or access to the system under certain conditions in order to combat an immediate heightened threat or to eliminate a disturbance. The RIA also has the right to carry out supervision, security audits, security checks, and to issue orders to stop illegal activities and to comply with the requirements of the law.
In the event of failure to comply with the RIA's order, a fine of up to 70,000 euros may be imposed.
In case of non-compliance with the requirements of the Cyber Security Act:

- critical entities are punished with a fine of up to 10,000,000 euros or up to 2% of the total global annual turnover of the critical entity of the previous financial year (whichever amount is greater);
- significant entities are penalized with a fine of up to 7,000,000 euros or up to 1.4% of the total global annual turnover of the significant entity in the previous financial year (whichever amount is greater).

Summary

The rapid development of technology makes cyber security an increasingly important field. In recent years, both the number of cyber-attacks and their complexity have increased in the European Union. Therefore, it is particularly important to achieve a higher level of cyber security throughout the European Union.
Check whether your company meets the characteristics of a service provider set out in Cyber Security Act and therefore falls within the scope of the law. If so, take all necessary measures to ensure your company's cyber security as soon as possible, but no later than three years after the law has entered into force.
In case you need any assistance with this matter, please do not hesitate to contact us!

Contact person

Alice Salumets

Attorney-at-Law
Partner

T +372 (6) 068 – 650

alice.salumets@roedl.com

Imprint

Publisher:
Rödl & Partner Estonia
Maakri 23 A 10145 Tallinn
info@roedl.ee
www.roedl.ee

Responsible for the content:
Marta Gromtsev
marta.gromtsev@roedl.com

Layout/Type:
Liisa Maide
liisa.maide@roedl.com