

# Rödl & Partner

## Transposition of the NIS2 Directive into national law – what is the current state in Estonia?

### NEWSLETTER

[www.roedl.ee/en](http://www.roedl.ee/en)



Dear reader,

Do you belong among companies which need to ensure their **cybersecurity** in the world of rapidly evolving technology resulting in heightened cybersecurity risks? If yes, then this Newsletter is for you.

#### **Transposition of the NIS2 Directive in Estonia**

The second version of the Network and Information Security Directive (hereinafter NIS2 Directive) entered into force in 2023. The NIS2 Directive is a vast legislation in the European Union which provides measures for higher-level cybersecurity. The NIS2 Directive stipulates a broader list of sectors subject to the foreseen updated measures and obligations compared to the original NIS Directive (hereinafter NIS1 Directive). Also, with NIS2 Directive, an updated sanctions regime for non-compliance is introduced.

The NIS2 Directive has not yet been transposed into Estonian law. In December 2024, the Government of the Republic prepared the relevant draft law to transpose the NIS2 Directive on a national level mainly by amending the national Cybersecurity Act. In addition, minor amendments to other relevant laws are planned with the draft law. Pursuant to the draft law, planned date for entry into force of the national law, transposing the NIS2 Directive, is July 1, 2025.

### **Companies subject to the NIS2 Directive**

First and foremost, the NIS2 Directive addresses medium and large companies. The NIS2 Directive differentiates between essential and important entities. Large companies are usually considered essential entities and medium-sized companies are usually considered important entities. For example, a large company with 250 or more employees and minimum annual turnover of 50 million is considered an essential entity.

However, the classification foreseen by the NIS2 Directive may vary – for example, small companies in the sector of public administration and medium-sized companies who provide public electronic communications service are considered essential entities. Also, in some cases, a company can be considered an essential or important entity regardless of its size, for example, in the sector of research.

Pursuant to the draft law, the amended Cybersecurity Act will be applicable to a company on two conditions:

- 1) exceeding the threshold set for numerical indicators (50 or more employees per year and annual turnover or balance sheet exceeding EUR 10 million), and
- 2) being active in a field listed by the law.

However, please note that the prerequisite for exceeding the threshold set for numerical indicators does not apply to some companies, such as essential service providers.

As a result of the NIS2 Directive, the Estonian draft law imposes *inter alia* the obligation of notifying relevant authorities of severe incidents on essential service providers and other sectors, for example, the sector of energy, waste, fuels, transport, finance, healthcare, ICT (information and communication technology), research, space, food (in the case of being active in wholesale, industrial production and processing) and public administration.

As mentioned above, the NIS2 Directive scope is broader. This means that companies, to which the Estonian Cybersecurity Act based on NIS1 Directive does not apply, may become subject to new requirements due to the transposition of the NIS2 Directive in Estonia. Thus, if your company has not been subject to the Estonian Cybersecurity Act so far, it is possible that the situation will change once the national law (transposing the NIS2 Directive) enters into force.

According to the Ministry of Justice and Digital Affairs, the state plans to introduce a tool to help determine whether companies are considered subject to the amended law. However, no further information on this is currently provided.

### **Sanctions in case of non-compliance with the law**

As of entry into force of the law transposing the NIS2 Directive, obliged companies will have 3 years to comply with cybersecurity requirements prescribed by the law(s). Pursuant to the draft law, in case of non-compliance, sanctions are set forth.

The NIS2 Directive prescribes that the sanctions shall be effective, proportionate and dissuasive. The sanctions foreseen in the draft law are notably higher compared to the sanctions in force as of today (today up to EUR 20 000).

Pursuant to the draft law, in case of non-compliance with the law:

- essential entities are punished by a fine up to EUR 10 000 000 or up to 2% of the global total annual turnover of the owner of the company (depending on which sum is bigger);
- important entities are punished by a fine up to EUR 7 000 000 or up to 1,4% of the global total annual turnover of the owner of the company (depending on which sum is bigger).

Due to Estonia's digital advancement, it is important that all Estonian companies subject to the requirements comply with them. In Estonia, many digital environments are in use, like the E-Business Register. Use of these digital environments needs to be secure.

If your company is active in the sector(s) subject to the new requirements, then fast action to incorporate necessary renewed technical and organisational approach is crucial as soon as possible but not later

than within three years as of the national law (transposing the NIS2 Directive) entering into force in July 2025.

Please note that this Newsletter is written on the basis of the draft law which means that final details will be made known as soon as the Riigikogu has passed the law.

In case you need any assistance with this matter, please do not hesitate to contact us!

Best regards

Alice Salumets  
Head of Office Estonia, Partner  
alice.salumets@roedl.com

[LinkedIn »](#) | [Facebook »](#)

## Imprint

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

**Responsible for the content:**  
Amanda-Nicoletta Sarros  
[amanda-nicoletta.sarros@roedl.com](mailto:amanda-nicoletta.sarros@roedl.com)

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

This Newsletter offers non-binding information and is intended for general information purposes only. It is not intended as legal, tax or business administration advice and cannot be relied upon as individual advice. When compiling this Newsletter and the information included herein, Rödl & Partner used every endeavour to observe due diligence as best as possible, nevertheless Rödl & Partner cannot be held liable for the correctness, up-to-date content or completeness of the presented information. The information included herein does not relate to any specific case of an individual or a legal entity, therefore, it is advised that professional advice on individual cases is always sought. Rödl & Partner assumes no responsibility for decisions made by the reader based on this Newsletter. Should you have further questions please contact Rödl & Partner contact persons.

The entire content of the newsletter and the technical information on the Internet is the intellectual property of Rödl & Partner and is protected by copyright. Users may load, print or copy the contents of the newsletter only for their own use. Any changes, duplication, distribution or public reproduction of the content or parts thereof, whether online or offline, require the prior written consent of Rödl & Partner.