



# Legal update

December 2023

# Weinhold Legal

## Contents

### Upcoming Legislation

The CSRD Directive

New act on cybersecurity

The information contained in this bulletin is presented to the best of our knowledge and belief at the time of going to press. However, specific information related to the topics listed in this bulletin should be consulted before any decisions are made.

#### **Banking, Finance & Insurance:**

Daniel Weinhold, Václav Štraser, Ondřej Tejnský

#### **Competition Law / EU Law:**

Tomáš Čermák

#### **Dispute Resolution:**

Milan Polák, Zbyšek Kordač, Anna Bartůňková, Michaela Koblasová, Michal Švec

#### **ESG – Environment, Social, (corporate) Governance:**

Daniel Weinhold, Tereza Hošková

#### **Family Office:**

Milan Polák, Zbyšek Kordač, Michaela Koblasová

#### **Insolvency and Restructuring:**

Zbyšek Kordač, Jakub Nedoma

#### **IT, Media & Telecommunication:**

Martin Lukáš, Jakub Nedoma, Michal Przewczek

#### **Labour Law:**

Eva Procházková, Anna Bartůňková, Daša Aradská, Ondřej Tejnský

#### **Mergers and Acquisitions:**

Daniel Weinhold, Václav Štraser

#### **Personal Data Protection**

Martin Lukáš, Tereza Hošková, Daša Aradská

#### **Public Procurement & Public Sector:**

Martin Lukáš, Tereza Hošková, Monika Švaříčková

#### **Real Estate:**

Pav Younis, Václav Štraser

#### **Slovak Law:**

Tomáš Čermák, Karin Konečná

#### **Start-ups, Venture Capital and Cryptocurrency:**

Pav Younis, Martin Lukáš, Jakub Nedoma, Michal Švec, Ondřej Tejnský

## Upcoming Legislation

### ESG reporting

Terms such as environment, sustainability, social inequality or transparency in corporate governance are becoming increasingly prevalent. These topics affect the society as a whole, which is why it is not surprising that the European Union is trying to address them in its legislation.

While certain steps have already been taken in the past, new steps are expected to have a much greater impact. One of them is one of the most discussed topics in the legal space at the moment - the upcoming changes in the area of ESG reporting.

Through ESG, it is possible to assess how a company is performing in three areas:

- 1) Environment – environmental impact, sustainability, emissions and waste reduction, energy efficiency;
- 2) Social – human rights, adequate working conditions, occupational health, diversity and
- 3) Governance – corporate governance structure, ethical and transparent management, combating corruption and preventing conflicts of interest.

By evaluating these criteria, a company can achieve an aggregate ESG score, which is useful not only for the company itself, but mainly for external parties (clients, investors, banks), who can more easily understand and evaluate ESG-related risks, thus gaining the opportunity to make informed decisions regarding any current or future cooperation with the company.

The ESG reporting obligation was first set out in the NFRD Directive, which was transposed into Czech law primarily by an amendment to Act No. 563/1991 Coll., on Accounting, as amended, with effect from 1 January 2017. However, its impact was very limited, as it imposed the obligation to disclose the above-mentioned information on only about 11,000 companies across Europe, while only about two dozen entities in the Czech Republic were affected.

As the NFRD Directive proved insufficient to achieve the desired objectives, the CSRD Directive was adopted instead, coming into force in January this year, with Member States being allowed until July 2024 to transpose it into their legal systems. The impact of the CSRD Directive will be much broader, with around 50,000 European companies, including over 1,000 Czech companies, now being subject to obligations.

The obligation to report information on the impact and risks of individual companies' activities in the areas of environmental, human rights and sustainability (ESG data) will now apply both to companies listed on regulated EU markets and to companies meeting at least two of the following three criteria:

- ▶ over 250 employees;
- ▶ balance sheet assets exceeding EUR 20 million;
- ▶ net turnover of more than EUR 40 million.



# Legal update

December 2023

## Weinhold Legal

However, it is also worth mentioning that even companies that do not meet these criteria themselves may still feel the impact of the ESG Directive if they are part of a supply chain. In this case, they will have to report data to larger entities within this chain.

Besides the significant expansion of the range of obliged entities, the areas of obligatory reporting are also an essential change. While the reporting obligation will only apply to the newly obliged entities over the course of the following few years, the changes introduced by the Directive will affect currently obliged entities as early as 2024. Companies will now be required to assess sustainability risks affecting society and to publish information with a focus on, for example, climate or human rights issues.

For this purpose, ESG data reporting standards were adopted on 31 July 2023, which, in addition to setting out specific data to report, are also expected to harmonise the currently widely varying quality of data reported by companies.

Although the changes may seem a long way off at the moment, it is more than advisable to start preparing for them now to avoid possible complications in the future.

### Cybersecurity according to NIS2

As the year nears to an end, the deadline for the transposition of the NIS2 Directive, which entered into force on 16 January 2023, is slowly approaching. Member States have until 17 October 2024 to adopt national legislation.

In the Czech Republic, the process of transposition began very early and the first draft of the new act on cyber security was published on the website of the National Cyber Security Bureau (NCSB) at the end of January 2023. During the year, the draft was amended by the suggestions of the expert and lay public and the NCSB expects to submit it to the government by early next year.

All obligations are therefore not yet known exactly, but the key ones can already be determined, including which entities will be newly subject to the minimum cybersecurity obligations of the NIS2 Directive. It is, however, at the discretion of Member States to determine additional obliged entities beyond the scope of the Directive, and it is therefore possible that this range will be extended.

The two main criteria for determining the future obliged entities and the extent of their obligations are (i) the sector and sub-sector in which the entity conducts its activities, and (ii) the size of the entity, to be understood in the sense of the European Commission Recommendation 2003/361/EC on the definition of micro, small and medium-sized enterprises. According to these criteria, the obliged entities shall be divided into two groups: a group of core entities falling under the higher obligation regime and a group of significant entities falling under the lower obligation regime.

The obligations should therefore apply to entities that meet the size requirement and are also active in one of the following sectors:

- ▶ energy;
- ▶ transport;
- ▶ banking and financial market infrastructure;
- ▶ healthcare;
- ▶ drinking water and wastewater;
- ▶ digital infrastructure;
- ▶ public administration;
- ▶ space and research;
- ▶ postal and courier services;
- ▶ waste treatment;
- ▶ manufacture, production and distribution of chemicals;
- ▶ food production, processing and distribution; and
- ▶ manufacture of medical devices, computers, electronic and optical instruments and electrical equipment and machinery, motor vehicles, trailers and semi-trailers and other transport equipment.

Although it is not yet possible to define the obligations exactly, it is possible to identify their scope to a certain degree. These will include, for example, the introduction of:

- ▶ active participation of top management in cybersecurity management;
- ▶ new managerial/accountability roles to ensure compliance of the obliged entity with its obligations;
- ▶ information security policies;
- ▶ contractual clauses to ensure security in the supply chain;
- ▶ cybersecurity training;
- ▶ security measures and procedures for evaluating their effectiveness;
- ▶ cryptography or information encryption;
- ▶ rules for managing access permissions;
- ▶ multi-factor identity verification, secure communication tools and emergency communication tools;
- ▶ rules for handling and reporting security incidents to NCSB or the operator of the National CERT;
- ▶ crisis management rules;
- ▶ rules for business continuity, backup and recovery in the event of a security incident.

Other than these obligations, it is also necessary to get an idea of what the obliged entities may be. In this regard, it should be highlighted that the entities will be required to carry out self-assessments and subsequently register under one of the two groups mentioned above (i.e. core and significant entities) on the NCSB portal.

According to the information currently available, the entity will have to comply with the registration obligation within 30 days from the date on which it has discovered that it meets the established criteria, but no later than 90 days from the actual fulfilment of these criteria.



# Legal update

December 2023

## Weinhold Legal

In addition, however, it is expected that some obliged entities will be determined directly by the state itself. In this case, the NCSB will directly communicate the obligation to the entity.

In accordance with the transposition deadline under the NIS2 Directive, the Cyber Law is expected to come into force in October 2024. It is therefore advisable to assess now whether and to what extent a given entity is likely to be subject to the obligations under the new legislation and to prepare for their implementation as soon as possible in order to avoid penalties, which the NCSB will be entitled to impose for non-compliance with these obligations from approximately November 2025 (or earlier in the case of a breach of the registration obligation) and which may include fines of up to CZK 250,000,000.

The information contained in this bulletin should not be construed as an exhaustive description of the relevant issues and any possible consequences, and should not be fully relied on in any decision-making processes or treated as a substitute for specific legal advice, which would be relevant to particular circumstances. Neither Weinhold Legal, s.r.o. advokátní kancelář nor any individual lawyer listed as an author of the information accepts any responsibility for any detriment which may arise from reliance on information published here. Furthermore, it should be noted that there may be various legal opinions on some of the issues raised in this bulletin due to the ambiguity of the relevant provisions and an interpretation other than the one we give us may prevail in the future.

Please send your comments to: [tereza.lavrincikova@weinholdlegal.com](mailto:tereza.lavrincikova@weinholdlegal.com) or contact the person you are usually in touch with. To unsubscribe from publications: [office@weinholdlegal.com](mailto:office@weinholdlegal.com)

© 2023 Weinhold Legal  
All rights reserved