WT Client Alert

Whistleblower Protection in Slovenia

Ensuring a management system in compliance with the Directive

15 February 2023

A law for whistleblower protection in the private sector was adopted in Slovenia, which introduces new requirements for internal compliance checks. Is your company ready?

The Slovenian Parliament has adopted the **Whistleblower Protection Act** ("**Act**") which will enter into force on 22 February 2023. The Act transposes the provisions of Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (the "**Directive**") into Slovenian law. Although the deadline for transposition has formally expired, Slovenia is far from being the only EU Member State to have missed the implementation deadline, as only 10 EU Member States have complied with this obligation so far.

Apart from new regulation of a whistleblowers' status and rights in the private sector, the Act also provides for an obligation to establish and maintain an internal system of whistleblower report verification. These new requirements significantly strengthen the responsibility of companies for their internal control of compliance, as has already been the practice of companies abroad for many years.

From a wider perspective, it may be as important as the proper implementation of the obligations under the Act that companies also conduct broader checks and comply with existing and binding sectoral regulations, including implementation of all the necessary internal policies and procedures.

1 What are the reporting procedures under the Act?

The Act provides for two channels through which whistleblowers (i.e. natural persons who report or publicly disclose information about a violation in a work-related context) can report violations, i.e. internal and external reporting channels.

The internal reporting channel should be the primary way of reporting. All legal entities employing 50 or more employees, as well as other entities engaged in certain specific activities, are required to set up internal reporting channels within the company. Private entities employing 250 or more employees are obliged to set up internal reporting channels within 90 days from the date of the entry into force of the Act, i.e. **by 23 May 2023**, while all others must comply with this obligation by **17 December 2023**.

The internally-submitted report is handled by an internally-appointed trustee who, after the procedure is completed, prepares an account of the findings on the merits of the report, the proposed and implemented measures and submits it to the management of the company and the whistleblower. The trustee must be an employee of the relevant company. Engagement of external contractors for this purpose is not allowed. The entities are obliged to

annually report the number of reports received, the number of anonymous and justified reports, and the number of retaliatory actions, to the Slovenian Commission for the Prevention of Corruption ("**CPC**").

Only companies employing less than 250 employees are allowed to share their resources for the receipt and investigation of reports with other group companies. The systems for receipt and investigation of reports that are now in place on a group level may not therefore comply with the Act.

Whistleblowers can use the external reporting channel in cases where the breach cannot be addressed effectively through internal reporting channels or if the whistleblower believes that there is a risk of retaliation in the case of an internal report. Depending on the nature of the breach, 22 different state institutions are responsible for receiving and handling the external reports (e.g. CPC, the Slovenian Securities Market Agency (*ATVP*), the Slovenian Competition Protection Agency (*AVK*), the Slovenian Insurance Supervision Agency (*AZN*), the Bank of Slovenia, the Agency for Medicinal Products and Medical Devices of the Republic of Slovenia (*JAZMP*), the Financial Administration of the Republic of Slovenia (*FURS*), inspectorates, etc.). When dealing with an external report, the relevant institution acts in accordance with the relevant sectoral laws and within its powers. In practice, this may result in the initiation of supervisory, inspection, administrative proceedings and, in extreme cases, even criminal proceedings.

2 Ensuring an efficient compliance system in accordance with the requirements of the Directive and the Act

For companies that are obliged to establish internal reporting channels under the Act, it is essential to set up and maintain an effective, independent and credible system for receiving and handling reports by whistleblowers, that are trusted by both employees and external stakeholders.

Such a system allows the company to identify and duly address any shortcomings before any state authorities or agencies may interfere with its operations and indirectly limits the number of external reports and related procedures that may significantly interfere with the company's day-to-day operations.

In view of the above, it is important that the company's existing policies are sufficiently specific in terms of both content and procedure to contain clear rules of conduct, responsibilities and action in cases of irregularities or breaches (e.g. on giving/accepting gifts, conflicts of interest, prevention of corruption, use of a company's email and telephone, storage of personal emails and documents, protection of personal data, prevention of mobbing, etc.).

3 Prohibition of retaliation against whistleblowers

Under the Act, any retaliatory action against a protected whistleblower, such as termination of employment, suspension of an employment contract, transfer to a lower position, preventing or withholding training or promotion, introduction of disciplinary proceedings, etc., is prohibited.

According to the Act, the whistleblower will not be considered to be in breach of any contractual or legal restriction or prohibition of disclosure of certain information (e.g. trade secrets) and will not be liable in connection therewith if the whistleblower did not report false information and believed that the report was crucial for the disclosure of the violation. Also, the whistleblower will not incur liability in respect of the acquisition of or access to information reported or publicly disclosed, provided that such acquisition or access did not constitute an independent criminal offence.

In the case of retaliation, the whistleblower may seek judicial protection before a competent court. If the whistleblower seeks an interim injunction in respect of retaliation measures taken against them and proves to have

made a report before the retaliatory measure was taken, the more onerous of the conditions to be fulfilled for an interim relief (i.e. that the enforcement of the claim will be prevented or substantially impeded) will automatically be deemed to have been fulfilled.

Furthermore, the damage incurred by the whistleblower will be deemed to have resulted from the retaliation and therefore, for instance, it is for the employer to prove that the employer's actions were legal, appropriate and not related to the report.

4 What are the consequences for breaching the new Act?

The Act distinguishes between systemic, minor and serious offences. Systemic offences refer to breaches of the obligation to establish an internal reporting channel, to appoint a trustee and to report to the CPC. Minor and serious offences refer to the disclosure of the whistleblower's identity and retaliation respectively. It should be noted that the Act explicitly criminalises the mere attempt or threat of such acts. The CPC will be responsible for conducting offence proceedings and for imposing penalties.

> **For serious offences, fines range between EUR 5,000 and EUR 20,000; EUR 10,000 and EUR 60,000 for companies** (depending on their size) and, additionally, between EUR 300 and EUR 2,500 for their responsible persons.

5 How can we support you?

Wolf Theiss offers the following integrated and tailored solutions to ensure business compliance, both in light of the Act and existing regulations:

(i) SecuReveal: a compliance tool — software-based reliable system for anonymous notification of irregularities in the company, which meets the highest data protection standards,
(ii) review of existing policies or drafting new internal policies for your company in order to establish an effective internal compliance system (e.g. policies on the use of the company's email and other communication systems, the use of work equipment and the storage of documents),
(iii) trainings for staff and management on compliance and on dealing with reports,
(iv) an experienced team of specialised lawyers covering various legal fields to manage and conduct more complex internal investigations within a company,
(v) coordination and communication with regulators and investigative authorities in the event of an external report, where unlike other advisers, we can offer both the facilities and the confidentiality of our legal services.

> In addition to our in-house expertise in employment law, personal data protection, as well as in corporate and white-collar crime investigations, **we also have the advantage of extensive international experience and effective cross-border cooperation when dealing with corporations with affiliated companies in Central, Eastern and Southeastern Europe.**

About Wolf Theiss

Wolf Theiss is one of the leading European law firms in Central, Eastern and South-Eastern Europe with a focus on international business law. With more than 360 lawyers in 13 countries, over 80% of the firm's work involves cross-border representation of international clients. Combining expertise in law and business, Wolf Theiss develops innovative solutions that integrate legal, financial and business know-how.

For more information, please contact:

Teja Balažic Jerovšek
Partner

E teja.balazic-jerovsek@wolftheiss.com
T +386 1 438 0024

Simon Tecco
Senior Associate | Odvetnik

E simon.tecco@wolftheiss.com
T +386 1 438 0037