

How to set up whistle blowing system in companies 2/28/22

Effective from 4 February 2022, the Whistle Blowing Act introduces new requirements compared to the earlier enactment with the same title, and takes over the provisions of Directive EU 2019/1937.¹ This article explores what a whistle-blowing system (WBS) really means in the light of the new Act and what options companies have for setting up such a system efficiently.

What is a whistle-blowing system?

The Act provides for several ways to blow the whistle:

- Setting up an internal WBS
- Reporting to a competent body
- Using a point of contact (trade union, foundation etc)
- Reporting publicly in certain cases

Setting up an internal WBS remains mandatory for everyone in the public sector under the new Act. In the private sector, the old enactment only placed this obligation on companies with a headcount of over 50. Currently the headcount criterion doesn't apply to companies operating in the financial and capital market sector or in preventing money laundering and the financing of terrorism and proliferation. So the new requirement effective from 4 February 2022 has expanded the range of companies that are required to set up an internal WBS.

It is important to note that the Act is not the only piece of legislation to lay down a reporting procedure because the Cabinet of Ministers has issued a rule² listing the pieces of EU legislation that provide for a different reporting procedure in certain areas.

What options are open to companies?

We wrote about the main requirements for an internal WBS in 2019. Although the requirements have been in force for three years now, our experience suggests that private businesses are relatively slow in setting up an efficient WBS for a variety of reasons. Some CEOs don't find the small penalties for breaching the Act to be motivating, while other CEOs feel unable to thrust more duties on their busy staff.

We see a WBS as an efficient tool to ensure your company stays compliant, as it allows you to identify potential breaches of law before supervisory bodies are involved or the information enters the public domain. So even companies that are not required to set up an internal WBS could benefit from doing so.

The requirements and principles governing an internal WBS basically remain unchanged, so it is still important for companies to adopt a system that efficiently provides a secure reporting environment, encouraging reporting as such and protecting the whistle-blower's identity and safeguarding them against potential adverse consequences.

Companies usually insert a WBS into their existing procedures, such as the code of conduct or employment manual, which might already provide for reporting breaches of the internal procedures. Accordingly, the employee who was responsible for processing reports on breaches of internal procedures is now also evaluating whistle-blower reports. Companies operating within a multinational group tend to apply their foreign-registered parent company's WBS unchanged. It is important to note, however, that different

member states have passed Directive EU 2019/1937 differently. For example, areas subject to whistle-blowing may be different. So it is the CEO's responsibility to check that the group's WBS meets Latvian requirements.

The market now offers electronic reporting tools that make the reporting process easier for the whistle-blower and may ensure full anonymity unless they wish to disclose their identity. However, the Act doesn't require companies to set up such an electronic tool, so they may adopt simpler methods of reporting, such as a separate reporting channel or email for whistle blowing or any other method that efficiently puts an appropriate process in place.

The Act currently permits a third party to ensure WBS operations, so some companies engage their consultants for this purpose. Since reports are examined by non-employees, using consultants can help your company create a more secure WBS. This mitigates the risk of jeopardising the whistle-blower's identity and causing them adverse consequences. And using consultants can give your management team more comfort that potential breaches of law included in the report will be evaluated independently, leading to an objective opinion.

¹ Directive (EU) 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

² The Cabinet of Ministers' Rule No. 96 of 8 February 2022, *Union law, breaches of which warrant whistle blowing or which provide for a different reporting procedure*