30yrs WARDYŃSKI+ PARTNERS

Whistleblowing system

A must-have or a nice-to-have?

March 2021

Introduction

Irregularities can occur even in the best-organised and -managed company. They can take different forms and have various consequences. Some of them interfere with business operations. Eliminating them can improve the organisation's operations and results. Others can expose the organisation and its managers to the risk of legal liability or endanger their reputation.

That's why it is vital to uncover irregularities as early as possible. Companies can deploy various tools to this end. They can retain external specialists to examine the company's organisation and operations. They can also turn to their own employees, who have the greatest knowledge of the organisation.

When employees are called on, they may be hesitant to speak up, particularly in the presence of others. Thus it is worthwhile to establish the appropriate culture of responsibility for the well-being of the company and to provide employees a convenient, confidential channel to report irregularities they may observe. The company must give a clear signal that all reports raised in good faith are important and will be considered.

More and more companies are deciding to introduce internal whistleblowing procedures. For now, except for listed companies, it is not mandatory to have such procedures in place, but that will soon change.

This is because the **Whistleblower Directive** (Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law) has been adopted at the EU level, and must be implemented by all EU member by 17 December 2021.

The obligation to implement internal reporting channels for breaches of EU law will apply to:

- **Legal entities in the public sector** (municipalities with fewer than 10,000 inhabitants or fewer than 50 workers may be exempted from this obligation)
- **All legal entities operating in the sectors of financial services, products and markets, and subject to regulations on prevention of money laundering and terrorist financing** (a detailed list of relevant EU laws is set forth in parts I.B and II of the annex to the directive)
- **Legal entities in the private sector employing 50 or more workers** (this obligation will first be imposed on entities employing **250 or more workers**, while regulations imposing this duty on entities employing 50–249 workers must be enacted by 17 December 2023)
- Potentially also **legal entities in the private sector employing fewer than 50 workers**, depending on a risk assessment taking into account the nature of the entities' activities.

The directive covers reporting of "breaches of Union law" (specific acts listed in the annex to the directive). It remains to be seen from the implementation into national law what approach the member states take to reporting of irregularities and protection of whistleblowers, and whether the national regulations extend to breaches of both EU and national law, or only certain laws or areas. However, it appears that the indicated categories of breaches of EU law will require the member states to implement these rules broadly.

Internal reporting channels—meaning what?

A whistleblowing procedure is not just a procedure and communications channel. It also means developing a whole set of organisational and procedural solutions that will:

- Instil a **culture of reporting irregularities**
- Create the **technical means for reporting irregularities** in a manner ensuring confidentiality
- Establish **mechanisms for verifying reports** and, if needed, protecting whistleblowers against retaliation.

Culture

In compliance principles, it is particularly important to "set the tone at the top," which means that board members and senior management must set an example and in their deeds must be engaged in creating a "culture of compliance," to help prevent prohibited behaviour by individuals and entities affiliated with the organisation (S.H. Deming, *Designing an effective anti-bribery compliance program: A practical guide for business* (ABA Book Publishing, 2018)).

Policies and procedures will only be effective if the managers of the organisation foster the right culture, and convince employees that they will take reports seriously and that whistleblowers will truly be protected against retaliation.

Channels

In practice, businesses introduce a wide range of solutions, from simple communiqués encouraging employees to report irregularities to their superiors, or boxes for submitting reports on paper, to more highly developed IT systems including special communications channels, teams designated to handle reports, and strict procedures for resolving complaints.

Selection of the right system for reporting irregularities depends primarily on the size of the organisation, the number of staff, the types of potential irregularities, and the corporate culture.

The directive sets minimum requirements that should be met by any system for reporting breaches of law. One of these requirements is **the need to keep the whistleblower's identity strictly confidential** (if the report is made under the whistleblower's name—the directive leaves it up to the member states' discretion how to regulate the issue of accepting and considering anonymous reports). This requirement will largely force businesses to abandon simpler solutions (such as a physical mailbox at the workplace or an employee's email) in favour of solutions offered by specialised suppliers (whistleblowing web-based platforms such as WhistleB, Navex, Lantero and others).

Protection of whistleblowers acting in good faith

Whistleblowers reporting breaches in good faith enjoy legal protection against retaliation. Currently this protection arises mostly under general regulations, and is largely elaborated through court decisions. Such protection also arises out of the Polish Constitution and the European Convention on Human Rights.

According to European case law, whistleblowers who are employees of the public or private sector, acting in good faith, are subject to protection. Their reports may involve classified or confidential information. But the information must be authentic, and the interest in having the information disclosed must not be outweighed by the damage suffered by the entity whose information is disclosed (see European Court of Human Rights judgments in *Guja v Moldova*, application no. 14277/04, *Heinisch v Germany*, application no. 28274/08, and *Marchenko v Ukraine*, application no. 4063/04). However, the only regulations in Poland expressly protecting whistleblowers are the new provisions on protection of business secrets.

The directive requires the member states to enact specific means for protecting whistleblowers against retaliation. Businesses introducing reporting systems should bear in mind the regulations on protection of whistleblowers acting in good faith. They should also protect against unwittingly allowing retaliatory measures by the employer or third parties, such as worsening of working conditions, demotion, reduction of salary, overlooking the whistleblower when awarding bonuses, termination, or defamation suits (e.g. filed by the perpetrator of the breach who is fired as a result of the whistleblowing).

In the case of large organisations with multi-level management in place, there is a risk that retaliatory measures might be taken against a whistleblower without the knowledge of senior management. In practice, such situations may arise when a lower-level worker reports objections to actions by a mid-level manager. If the mid-level person learns of the report and identifies the whistleblower, he might abuse his power and access to senior management's ear to recommend that the lower-level employee be fired due to poor results, failure to integrate with the team, or the like.

What benefits come from having a whistleblowing procedure?

A frequent reason for adopting a whistleblowing procedure, even when it is not yet required, is the desire to learn about problems internally, rather than from outside sources such as the press, employee websites, social media, or, worse, state authorities.

An employee or associate with no one to turn to in the company with a problem may become more and more frustrated and thus decide to disclose negative information about the company on the internet or to the competent authorities, such as the State Labour Inspectorate or law enforcement.

If the company learns of irregularities first, it can remediate the problem, punish the infringer, and improve the organisation to avoid similar irregularities. Moreover, having reporting channels in place increases the odds of discovering problems faster, at an earlier stage—before the negative consequences grow truly serious.

Directive 2019/1937 is not the first legislative initiative introducing regulations on reporting of irregularities and protection of whistleblowers. Public companies already have a legal obligation to introduce systems for reporting irregularities (under the Public Offerings Act). There are also other bills proposing to introduce such a legal requirement, in particular the proposed new act on corporate criminal liability (work on which was interrupted when the parliamentary term ended but is likely to be resumed).

> *Regarding private companies, the inception impact assessment states that implementing internal whistleblowing arrangements can help avert or address reputational and economic risks and damages, deliver high standards of public and customer service and gain trust amongst consumers and investors. The inception impact assessment further sets out the likely positive impacts of EU action on whistleblower protection on employees and the environment.*
>
> – J. T. Stappers, EU Whistleblower Protection Directive: Europe on Whistleblowing

The article also cites studies finding that organisations with whistleblowing channels uncover fraud faster (on average within 12 months) than those without a system in place (on average within 18 months).

How should a reporting system look?

To enable whistleblowers to effectively report irregularities, an appropriate system needs to be created providing for a procedure to be followed by whistleblowers and by persons following up on their reports.

Under the directive, the whistleblowing system must:

- Indicate relevant channels or methods for submitting reports (in writing and orally, whether by telephone or in person)
- Ensure protection of the whistleblower's identity (and also ensure the possibility of reporting anonymously, if that solution is adopted)
- Designate a person or division (depending on the size of the entity) to follow up—to verify the report and take further actions, such as collecting supporting evidence
- Ensure that follow-up measures are taken in compliance with principles of due diligence, confidentiality and impartiality
- Ensure that whistleblowers receive confirmation of receipt of their report within seven days, and feedback on how the matter has been handled within three months
- Provide clear and easily accessible information on how and where to report
- Ensure that no retaliation is taken against whistleblowers.

Regardless of the reporting channel (email, telephone, in person, via dedicated software, etc), the selected system must ensure the confidentiality and security of the information reported and the whistleblower, and also prevent unauthorised access to the information.

Reports must also be registered (e.g. through recording, transcription, meeting minutes, in electronic form, etc), so that the reports are stored and their existence can be confirmed.

You've implemented a reporting system—now what?

A reporting procedure is not just a set of formal rules. It's also a question of corporate culture. An organisation implementing a reporting system must ensure that all staff are familiar with the system—know how to report problems and know their rights. The employer should encourage employees to exercise the possibility of reporting irregularities, and should also clearly demonstrate that whistleblowers will not suffer retaliation and will be protected by the employer.

What about when the organisation receives a report from a whistleblower? **The best place to start is an action plan, which should answer four basic questions:**

1. Who (inside and outside the company) should be notified of the matter?
2. Who will verify the allegations, and in what manner?
3. How big is the risk that if the allegations are upheld, the company will be exposed to legal liability or loss of reputation—and what can be done to minimise the risk?
4. Is the company prepared to cooperate with state authorities, if they decide for example to conduct an inspection or search at the company?

The business should maintain a **record of reports** and assign analysis of reports to trusted employees with appropriate seniority in the organisation. The point is that the persons analysing reports should have the relevant competence, experience and position to appropriately verify and investigate the report. The system should prevent conflicts of interest. It is essential for the management board to have ready access to the record of reports (except for reports involving board members). The board should also receive regular reports on the number of whistleblower complaints received and how they are verified and resolved.

The aim of an internal investigation is to determine:

- Whether a breach has occurred
- The cause of the breach, including factors creating an environment conducive to the occurrence of irregularities
- The actual or potential consequences of the breach for the organisation and staff
- Who is responsible for the breach

Essentially, reports should be investigated, and if the allegations are confirmed, the irregularities should be eliminated. If certain employees are responsible for their occurrence, the employer may impose appropriate consequences (e.g. a reprimand or even disciplinary termination). In the case of irregularities arising out of structural and organisational problems, the business should take remedial action to eliminate the root cause.

The business should regularly check that the reporting system is effective, complies with current legal requirements, and is properly implemented. An absence of reports might suggest that the company is functioning properly, but could also be because the reporting system is dysfunctional and requires improvement. To this end it is a good practice to assign a "whistleblower champion" to evaluate the effectiveness of the system on a regular basis.

Once a reporting system is in place, the organisation must take a serious approach to analysing any reports received. Once a report enters the system, the company will hardly be able to defend itself in criminal, civil or administrative proceedings by claiming that the company or the management board was "not aware of the problem." Even if the board can truly say that they did not read the reports, it would be easy to claim that the board did not exercise due care. The record and content of reports are often obtained by law enforcement authorities, market regulators, and adversaries in litigation. And in the case of transactions involving the company, these materials will be subjected to detailed analysis during the due diligence process.

.

Summary

The Whistleblower Directive is already in force, and Poland has until 17 December 2021 to implement it into national law (or 17 December 2023 in certain respects).

The directive sets the aims as well as minimum standards for protection of whistleblowers and reporting systems, which as a rule will be mandatory for public legal entities and for private legal entities employing 50 or more people. The specific shape of the requirements in Poland will be known soon. But organisations can already start preparing for implementation of whistleblowing systems.

* * *

Contact

Łukasz Lasek
adwokat, partner

lukasz.lasek@wardynski.com.pl

Szymon Kubiak
attorney-at-law, partner

szymon.kubiak@wardynski.com.pl

Team

Maria Kozłowska
adwokat

criminal law

Katarzyna Żukowska
adwokat

data protection

Katarzyna Magnuska
attorney-at-law

employment

Wardyński & Partners
Al. Ujazdowskie 10, 00-478 Warsaw

Tel.: +48 22 437 82 00, 22 537 82 00
Fax: +48 22 437 82 01, 22 537 82 01
E-mail: warsaw@wardynski.com.pl