

DLA Piper Poland

Guide for Employers: Whistleblowing in Poland

Whistleblowing

The implementation of whistleblowing procedures is not only a response to EU Directive 2019/1937, but also an important part of building a culture of transparency and ethics within an organisation.

This guide aims to help employers understand the new regulations proposed in the latest bill and prepare them to implement the relevant procedures.

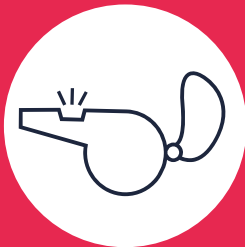
Scope and purpose

The latest bill requires all entities, both public and private, that employ **at least 50 people** to implement internal whistleblowing procedures. This number includes people working under employment contracts and those working under other legal bases, such as civil law or B2B contracts. **Entities with fewer than 50 employees may voluntarily implement procedures.**

However, the above threshold does not apply to legal entities conducting financial, transport safety and environmental protection activities - all of these entities, regardless of how many people they employ, are required to have an internal whistleblowing procedure in place.

An interesting solution that is possible for private entities employing between 50 and 249 people is for them to jointly establish rules for the acceptance and verification of internal whistleblowing reports and the conduct of investigations.

In addition, private group entities will be able to establish a joint procedure for internal reporting, provided that the activities performed are in compliance with the law. Solutions of this type can help many entities reduce paperwork and increase the efficiency of group policies.



Who is a whistleblower?

A whistleblower is an individual who reports irregularities in the operation of an organisation. They can be employees, temporary employees, individuals working under civil law contracts, entrepreneurs, proxies, shareholders, interns and others.

Spectrum of reportable cases

The subject of reports can be any observed or suspected breaches of the law that may be occurring within the organisation. This covers a wide range of potential irregularities including, but not limited to:



Corruption and financial crime: all forms of corruption, including bribery, fraud, financial embezzlement, or irregularities in financial management.



Data protection: breaches of data protection legislation, in particular breaches of the GDPR.



Public procurement: irregularities in tendering processes and the unlawful awarding of public contracts.



Competition violations: actions restricting competition and breaches of antitrust law.




Product safety: issues relating to the non-compliance of products with safety standards, which may pose a risk to consumers.



Environmental issues: breaches of environmental legislation, inadequate waste management, and environmental pollution.



Consumer protection and financial markets: irregularities concerning the protection of consumer rights, or abuses in financial markets.



Reports may concern illegal acts as well as unethical activities that, while not always constituting a breach of the law, may be harmful to the organisation or society. Whistleblowers are encouraged to report any suspected breaches in order to ensure compliance with the law and ethical and transparent practices within the organisation.

Elements of the internal reporting procedure



Receiving entity: this can be an internal organisational unit or person within the company's organisational structure, or an external entity authorised to receive internal reports.



Protection of whistleblowers: there should be procedures to protect whistleblowers from any form of retaliation, including bullying, discrimination or unfair treatment in the workplace.



Reporting channels: clear and easily accessible channels for submitting information must be indicated, such as dedicated email addresses, secure online forms, and telephone numbers.



Information obligations: a whistleblower must be provided with acknowledgement of the receipt of his/her report within seven days of it being made. Feedback on each report must be provided within three months of this acknowledgement.



Data protection: there should be rules on the protection of the personal data of whistleblowers and data subjects that are compliant with the GDPR.



Anonymous reports: there should be a procedure for dealing with anonymous reports.



How to handle a report: an entity within the organisation that is authorised to take follow-up action must be indicated. There must be a description of the procedure for handling a report, including the first steps upon receipt of the report, the investigative methods, and the response time. This function can also be performed by the entity receiving the report as long as impartiality is ensured.



External reports: clear and easily accessible information must be provided on how to make external reports to the Commissioner for Human Rights or public authorities and, where appropriate, to European Union institutions, bodies or agencies. It is worth noting that under the latest bill, this obligation will come into force three months later than the obligation to establish the internal reporting procedure itself.

Implementing the procedure

The implementation of the internal reporting procedure should be consulted with the company's trade union organisation or, if there is no such organisation, with the elected representatives of the employees. If there are no such representatives, the company should organise an election. The consultations should last between 5 and 10 days and the procedure itself enters into force seven days after being communicated to the employees.



Training and awareness

The organisation should provide regular training to all its employees, informing them of the procedures, the rights of whistleblowers, and the protection that the system offers.



Monitoring of procedures

Whistleblowing procedures should be regularly reviewed and updated to ensure that they are effective and comply with applicable law. It is also one of the employers' responsibilities to keep a record of internal reports.



Keep in mind

Anonymous reporting of breaches:

employers can decide to accept anonymous reports, but they must establish procedures for dealing with such reports, as required by the law.

Free legal aid for whistleblowers:

the latest bill includes provisions ensuring that whistleblowers have access to free legal aid, which includes legal support provided by the state in accordance with the Act on Free Legal Aid and Citizens' Advice and Legal Education.

Ban on retaliation: whistleblowers are protected from retaliation, which may include, but is not limited to, termination of employment, reduction of remuneration, blocking of promotions, harassment, discrimination, as well as other forms of unfair treatment. Any form of reprisal for making a whistleblowing report is prohibited, which includes negative consequences related to the whistleblower's career and finances.



Sanctions

A whistleblower who has been the victim of retaliation has the **right to compensation** of an amount not lower than the average monthly wage in the national economy in the previous year, or the right to damages.

In turn, a person who has suffered damage due to a whistleblower knowingly reporting or disclosing untrue information to the public is **entitled to compensation and damages for the violation of personal rights from the whistleblower** who made the report or public disclosure.

The latest bill also provides for **criminal penalties** for preventing or obstructing a whistleblower from reporting, retaliating against a whistleblower, revealing the identity of a whistleblower, making false reports, failing to establish an internal reporting procedure, or establishing an internal reporting procedure in violation of the law. The penalties are: a fine, a restriction of liberty, or imprisonment for up to three years.



Deadline for implementation

The most of the provisions, **including the obligation to implement an internal reporting procedure**, are to take effect three months after the date on which the new act is published in the Journal of Laws. In order to give organisations and public bodies more time to prepare to meet specific requirements, **the bill provides for a longer deadline of six months** for the entry into force of certain provisions.

Data protection

- Drafting and adopting privacy policies and privacy notices
- Compliance with mandatory data retention periods
- Protecting information about the identity of the whistleblower
- Performance of the Data Subject Rights, including in particular data access right and right to obtain a copy of the data and rules of the proceedings and protection of the whistleblower
- Ensuring compliance with GDPR provisions when entrusting data to an external service provider (especially in the case of international data transfers).



Data retention periods

The Polish law introduces mandatory periods for which personal data related to a whistleblower's report must be retained:

- 3 years after the end of the calendar year in which:
 - the follow-up actions or
 - the proceedings initiated by these actions have been completed or
 - the external notification has been transmitted to a public authority.
- 14 days after the determination that they are not relevant to the case in a situation of accidental collection.



Protecting information about the identity of the whistleblower

The Polish law introduces an exemption to the provisions of the GDPR to the extent that their application could lead to the disclosure of the identity of the whistleblower to the person to whom the report relates (unless the whistleblower expressly consents to the disclosure of his or her identity):

- Information obligation - exemption from the obligation to inform about the source of the data.
- Data subject's access right - exemption from the obligation to provide information about the source of personal data.



Information obligation

- Multi-stage communication may be applied.
- In the first stage, when introducing the whistleblowing procedure, information on the procedure and the privacy policy regarding the data collected should be provided to employees.
- In the next stage, detailed information on the processing of data in relation to a specific notification should be provided.



Checklist

Before introducing a whistleblowing system in an organisation, employers should consider the following issues to ensure that procedures are effective and compliant with the law:

1. Review the current procedures - do they meet the new requirements?
2. Has there been mandatory consultation with trade unions or employee representatives to obtain their support and comments on the procedure?
3. Decision on the form of implementation: will the procedure be implemented as a separate system for each entity in the group or as a common system covering several entities?
4. Selection of the responsible entity: who will be responsible for processing and examining reports? Will it be an internal organisational unit or an external service provider?
5. Develop a data protection policy - make sure procedures are in line with the GDPR.
6. Protecting anonymity and confidentiality: what mechanisms have been put in place to protect the anonymity of whistleblowers and the confidentiality of the information provided?
7. Accessibility and comprehensibility of procedures: are the procedures clear and accessible to all those entitled to report, including employees at different levels of the organisation?
8. Training for employees: what training will be provided to ensure that employees are aware of the new procedures and their rights under the reporting system and how often will it take place?
9. Monitoring and evaluation of effectiveness: what mechanisms have been planned to regularly monitor the effectiveness of the procedures and to make any necessary updates or corrections?
10. Promote the procedures within the company - how will employees be informed and encouraged to participate?

Conclusion

The implementation of an effective whistleblowing system is not only a legal requirement, but also a key element in building a transparent and accountable organisational culture. It is recommended that employers approach this task strategically, involving all levels of the organisation and ensuring that procedures are understandable, accessible and effective.

Contact

Employment



Agnieszka Lechman-Filipiak

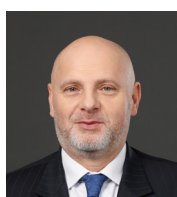
Partner | Head of Employment
agnieszka.lechman-filipiak@dlapiper.com



Michał Synowiec

Partner
michal.synowiec@dlapiper.com

Compliance



Tomasz Rudyk

Partner | Head of Compliance
tomasz.rudyk@dlapiper.com



Magdalena Dec

Counsel
magdalena.dec@dlapiper.com

Privacy and data protection



Ewa Kurowska-Tober

Partner | Head of IPT
ewa.kurowska-tober@dlapiper.com



Karol Kuterek

Junior Associate
karol.kuterek@dlapiper.com

