AGNIESZKA GODUSŁAWSKA
adwokat, Employment practice

AGNIESZKA LISIECKA
adwokat, partner heading the Employment practice

How to prepare for implementation of whistleblower regulations?

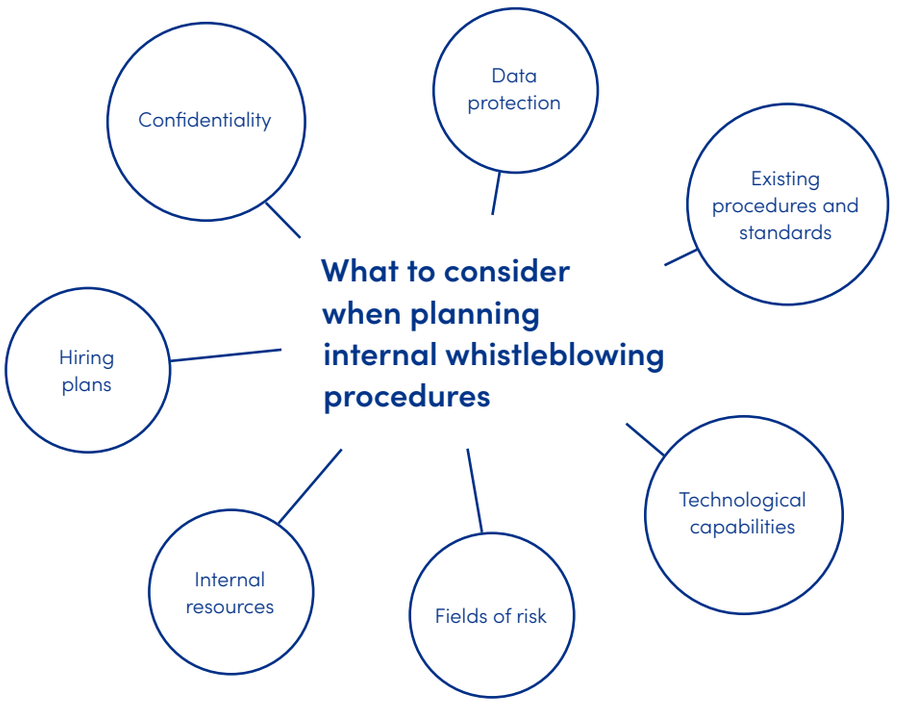
The deadline has passed, but the regulations are not yet in place. Businesses should take advantage of the delay to think through all aspects of their internal whistleblowing procedures.

The deadline for implementation of the EU's Whistleblowing Directive (2019/1937) passed over a year ago, but regulations implementing the directive into the Polish legal system have yet to be adopted. Over the course of the year successive drafts were circulated, but it is hard to resist the impression that the pace of work on the side of the government has slowed to a crawl.

Although the final wording of the Polish regulations is not yet known, it is worth considering the key issues in due time from the perspective of future compliance. This is particularly important in the case of undertakings employing 250 or more people, which will be first group required to implement internal whistleblowing procedures.

Private entities employing 50–249 people will have more time to implement whistleblowing procedures, but the deadline is still fast approaching (under the directive, the deadline for this group of undertakings is 17 December 2023).

In this article we discuss the main areas for functioning of internal reporting channels which require organisations to take implementation decisions, and which they can already start considering. »



What will be reported?

All indications are that entities implementing whistleblowing procedures will be able to expand the set of infringements that can be reported to include not just breaches of EU law as referred to in the directive, but also infringements of internal regulations or ethical standards in force within the organisation. This possibility has been included in all drafts so far of the act implementing the directive into Polish law.

However, the decision to include infringements of internal rules and ethical codes in the whistleblowing system should be carefully considered, as such complaints will require follow-up and internal proceedings under the same rules as infringements in other areas.

So it is worth analysing the enterprise's internal procedures and ethical codes now in light of the matters regulated there, as well as the level of detail of these rules. Often ethical codes define standards of behaviour in many areas, and the standards are often vague and general, and thus can be hard to enforce in practice.

At the same time, ethical codes in force at businesses often contain provisions banning discrimination and mobbing. So if they are included in the whistleblowing procedure, the internal reporting channels can morph into a tool for considering individual complaints by employees and associates. This in turn will require businesses to commit greater human and operational resources to consideration of such complaints. Meanwhile, many employers have already implemented separate anti-mobbing procedures. Therefore, before deciding on the areas to be covered by the whistleblowing procedure, employers must also review their internal anti-mobbing procedures and adjust them accordingly (which sometimes may mean having to repeal them entirely), to avoid any conflict in the internal standards at the organisation in this respect.

Who will receive complaints?

A basic challenge for companies is to ensure that the reporting channels function efficiently, and ensure independence and confidentiality. How these channels function will depend on whether people with knowledge of irregularities—potential whistleblowers—decide to report them.

Businesses may designate an internal unit or person within the entity's own organisational structure to receive complaints. However, the directive permits delegation of the duty to receive reports to external entities via outsourcing. Such third parties designated to receive complaints may be providers of tech platforms and solutions for submitting complaints, external advisers, auditors, or even employee representatives.

The decision to use the organisation's own channels or external reporting channels should be preceded by an analysis of the organisation's own capabilities and resources (particularly personnel), the tech solutions and tools offered on the market and the related costs, as well as the additional obligations and risks associated with delegating these tasks to external providers.

External entities hired to handle whistleblowing systems must have appropriate security measures in place and meet certain requirements, in particular involving protection of the safety and confidentiality of whistleblowers and persons identified in the report, as well as protection of other data included in the report, against unauthorised access.

Delegation of receipt of whistleblowing reports to an external organisation will require conclusion of an agreement with the external service provider, and compliance with a range of duties under the regulations on protection of personal data. Businesses

must remember in this regard that they bear responsibility for potential breaches by the external entity receiving whistleblower complaints. In particular, it is worth considering securing issues related to violation of confidentiality by including appropriate contractual penalties in the contract with the external service provider.

Which tech solutions?

Under the directive, whistleblowing channels must allow complaints to be made in writing or orally, but it is up to the organisation to decide which type of channel to establish.

Written complaints may be made in traditional or electronic form (e.g. by email). It is also worth considering the possibility of using other tech tools and solutions, e.g. systems specially created for this purpose or various types of messaging services available on the market.

In turn, oral reporting may be done by telephone or other voice communication systems. It should be considered whether the hotline for whistleblowers will be accessible around the clock or only during scheduled hours. While written complaints, particularly in electronic form, can easily be submitted at any time, it will be harder for businesses to ensure constant access to personnel receiving telephone calls from whistleblowers. It would seem to be simpler to use other voice communication systems, such as voicemail, which by their nature do not require the involvement of individuals receiving complaints live in real time.

At the request of the whistleblower, there should also be an option to receive the report via a face-to-face meeting scheduled within a reasonable time. This seems like an attractive form to use, as it allows whistleblowers to present evidence to back their claims, and when needed, for the organisation to clarify certain issues via dialogue between the whistleblower and the person receiving the complaint. But for businesses this will require training of individuals receiving complaints in this form.

Who will follow up?

When a complaint is made, that is the first step, setting off the whole procedure for internal reporting. The next stage (after confirming to the whistleblower that the complaint has been received) is to take follow-up actions. These are aimed at assessing the truth of the allegations raised in the report, and if the breach has not yet occurred, to respond and prevent the breach from occurring.

The next challenge to be met by private entities is thus to designate an individual or unit for taking follow-up actions in connection with a complaint. Selection of the most appropriate person or persons will be determined by the organisation's own structure, the sector in which it operates, and the scale and type of potential breaches. It is worthwhile to identify at the start the risk factors and areas relevant to the organisation's business profile. For example, in the case of entities from the banking sector, a potential risk area would include the assessment of customers' credit capacity and lending decisions, a stage where internal or external pressure might be brought to bear.

In any case, the person designated to take follow-up measures should provide assurances of impartiality, independence, and freedom from conflicts of interest.

It should be pointed out that persons designated to receive complaints may also conduct the follow-up.

Channels for reporting and verification—the organisation's own, or shared?

Entities from the private sector employing 50–249 workers may also decide whether they wish to use exclusively their own in-house channels for reporting and follow-up, or share such resources with other entities. The directive allows this group of entities to create shared channels for receiving reports and conducting investigations. This sharing of resources requires a separate agreement between the entities involved.

Creation of shared channels for reporting and investigation may be particularly suitable for corporate groups where a common hotline or even an entire compliance division examining internal complaints is nothing new, but has been rooted in the corporate culture for a long time. Such solutions are often dictated by the need to ensure consistent standards across the entire group.

Significantly, the directive does not exclude the possibility of creating and using cross-border channels for reporting and follow-up. But the use of international reporting channels may pose serious practical difficulties, primarily arising from the different regulations governing

At the request of the whistleblower, there should also be an option to receive the report via a face-to-face meeting scheduled within a reasonable time.

Entities employing 250 or more workers are not allowed to use shared resources for reporting and investigation.

whistleblowing procedures at the national level. A separate question is the duty to ensure that the operation of a shared hotline and investigative resources by one (common) entity complies with the data protection regulations. The proposed provisions on this issue in the draft Whistleblower Protection Act in Poland raise many doubts (beyond the scope of this article).

In considering the possibility of using shared channels for reporting and investigating complaints, businesses must take into account the number of employees and associates, as well as planned changes in this regard. Entities employing 250 or more workers are not allowed to use shared resources for reporting and investigation. Thus a rapidly growing enterprise may be able to use shared resources only for a short time, so efforts to arrange shared resources in such cases may not make sense.

Summary

Advance consideration of the model for the internal reporting procedure within the company will allow for efficient implementation of the procedure and completion of other related formalities (including under data protection rules) when the Polish parliament gets around to adopting regulations on whistleblower protection. Well-thought-out and well-functioning procedures should encourage people with knowledge of potential violations to come forward and report breaches.

Smooth adoption of an internal reporting procedure will also allow more time for training people responsible for receiving complaints and conducting follow-up. This in turn will help ensure compliance with the regulations and investigation of complaints in accordance with principles of independence and confidentiality, and protection of both whistleblowers and the persons mentioned in complaints, thus limiting the business's exposure to claims by the persons concerned.