PEARLE
Live Performance Europe

The Whistleblower Directive: all you have to know on employers' responsibilities

BRIEFING NOTE

Ref P8171

February 2023

Introduction – what is it about?

In October 2019, the European Commission for the first time, protected whistleblowers across the EU when adopting Directive (EU) 2019/1937. The new law is meant to **guarantee a high-level protection for whistleblowers who report on breaches to EU law by establishing safe report channels**, both within an organisation and to public authorities. It also protects whistleblowers against dismissal, demotion and other forms of retaliation.

The adoption of the Whistleblowers Directive followed a series of high-profile disclosures relating to scandals such as Cambridge Analytica, the Panama Papers and LuxLeaks. The new legislation had to be implemented by Member States into national law by **17 December 2021**, however, many EU countries failed to implement it on time.

The Directive is an attempt to improve whistleblowers' protection and, given the potential cross-border nature of the reported breaches, it aims at creating a unified legal framework in Europe.

The new rules have potential effects on our sector. For example, in the area of public procurement as regards renovation of buildings, this Directive could apply in case of breach of EU law. It could also have an effect if someone were in position to disclose breaches of EU law concerning the respect for privacy and protection of personal data. For example, someone disclosing information concerning consumer's data not processed with due regard for European data protection rules (the GDPR) could be protected under the whistleblower Directive.

Who is a whistleblower? (Article 4)

The European Commission defines whistleblowers as "people speaking up when they encounter, in the context of their work, wrongdoing that can harm the public interest, for instance by damaging the environment, public health and consumer safety and EU public finances".

How does the situation on whistleblowing look like in the EU today?

Before the EU adopted the Whistleblower Directive, ten EU countries (France, Hungary, Ireland, Italy, Lithuania, Malta, Netherlands, Slovakia, Sweden and United Kingdom) protected whistleblowers through national law schemes. The new Directive sets new standards and aims at harmonising rules which for the moment are fragmented and uneven across policy areas.

In December 2021 – deadline for Member States to transpose the Directive – the Brussels' online magazine Euractiv reported that most of the Member States had failed to transpose the Directive on time.

To know more about the transposition in your own country, check out the EU Whistleblowing Monitor: https://www.whistleblowingmonitor.eu.

Scope of the Directive (Article 2)

The Directive sets minimum standards to protect persons who work for a public or private organisation or are in contact with such an organisation in the context of their work-related activities and who report about breaches of Union law. The concerned areas of EU law include:

- Public procurement;
- Financial services, products and markets, and prevention of money laundering and terrorist financing;
- Product safety and compliance;
- Protection of the environment;
- Consumer protection;
- Protection of privacy and personal data, and security of network and information systems;
- Breaches relating to the internal market, including breaches of union competition and state aid rules.

The full list of the concerned areas can be found on this following website: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3442.

Who is covered by the Directive and can report as a whistleblower? (Article 4)

The Directive covers a wide variety of persons that may report in a work-related context. The work-related context must be interpreted broadly.

- Workers, including civil servants;
- Shareholders and persons belonging to the administrative, management or supervisory body of an undertaking;
- Self-employed workers;

- Any persons working under the supervision and direction of contractors, subcontractors and suppliers;
- Non-executive members, as well as volunteers and paid or unpaid trainees;
- Job applicants;
- Persons whose contracts have ended and who are not working any-longer for the undertaking.

Furthermore, protection should be provided to others who can experience (indirect) retaliatory measures due to a report. Such persons may include facilitators, colleagues or relatives of the reporting person.

A person should be able to report internally, meaning within an organisation or legal entity, as well as externally, to the competent authorities. Both are included within the scope of the text. The Directive encourages to report internally before reporting externally, when the reporting person considers that there is no risk of retaliation.

Which organisations or companies have to set up such reporting channels? (Article 8)

The scope of the Directive is very broad. It applies to **public and private organisations and companies across all sectors**.

For the private sector, there is an **exemption for SME with under 50 workers**. However, Member States can encourage these small entities to also provide reporting channels with less requirements than listed in the Directive.

Companies in the private sector with 50 to 249 workers benefit from a potential extra time of two years to set up the reporting channels – depending on national transposition. The Directive allows Member States to take more time to transpose the provisions concerning such companies, until 17 December 2023.

For the public sector, the establishment of channels is mandatory for all legal entities, including any entity owned or controlled by such entities. However, **Member States may exempt from this obligation public entities with fewer than 50 workers.**

Depending on the national transposition of the Directive, it might be possible for certain public entities to share internal reporting channels, provided that the shared internal reporting channels are distinct from and autonomous in relation to the relevant external reporting channels. As regards companies in the private sector with 50 to 249 workers, they may share resources concerning the receipt of orders and any investigation to be carried out.

In concrete terms, it means that, for our sector, several theatres, opera houses, live venues or other live performance organisations could join forces to set up the reporting channels.

What do organisations and companies need to do to comply with EU law?

1. **Organisations and companies must design and implement internal reporting channels (Article 9)**

In the set up of their internal reporting channels, a dedicated person or department should be appointed in order to handle incoming reports and follow-up thereon. Such reporting channels should allow reports to be made orally or in writing. The choice of the most appropriate persons or departments within a legal entity in the private sector to be designated as competent to receive and follow up on reports depends on the structure of the entity, but, in any case, their function should be such as to ensure independence and absence of conflict of interest.

As regards our sector, and more specifically for smaller entities, this function could be a dual function held by a company officer well placed to report directly to the organisational head, such as a chief compliance or human resources officer, an integrity officer, a legal or privacy officer, a chief financial officer, a chief audit executive or a member of the board.

The internal reporting channel has to be designed, established and operated in such a manner that it:

- Provides for anonymous reporting if this is allowed under national legislation;
- Protects the identity of the reporter and parties mentioned in a report;
- Is not accessible for non-authorised staff members;
- Provides for diligent follow-up on the report by a designated person or department.

2. **Organisation and companies must provide potential reporters with clear and accessible information on external reporting to the competent national authorities (Article 9)**

According to Article 9(1)(g), when an internal reporting channel has been created in a company or an organisation, it must provide clear and easily accessible information regarding the procedures for reporting externally to competent authorities (for instance via a whistleblower hotline) and, where relevant, to institutions, bodies, offices or agencies of the Union.

Each Member State must establish independent and autonomous external reporting channels. Concretely, Member States must designate a specific authority competent to receive, give feedback and follow up on reports. Member States should ensure that the competent authority provides feedback to the reporting person within three months (six months in duly justified cases).

In France, in the course of the national implementation of the Directive, the government provided a list of national authorities that have to establish external reporting channels (for example for the respect for privacy and protection of personal data: ‘Commission nationale de l’informatique et des libertés’ and the ‘Agence nationale de la sécurité des systèmes

d'information'). These authorities must respect a certain number of procedural and information obligations. This includes the obligation to publish on their website, in a section created on purpose, information about the external reporting channels and the conditions to be able to qualify as a whistleblower. For example, in the 'Commission national de l'informatique et des libertés', the potential whistleblower can either send a letter to the agency or use an internal electronic platform or communicate by phone with the agency.

3. Organisations and companies must follow-up on reports (Article 9)

In addition to implementing and/or improving an internal reporting channel, the Directive requires an **acknowledgement of the receipt** of a report towards the person reporting within 7 days. Also, **further feedback** to the reporter must be provided within a reasonable timeframe (at least within 3 months) after the receipt of the report. Note that Member States can implement even stricter measures with shorter timeframes.

Furthermore, organisations are required to **register incoming reports adequately** and in a secure manner. All report-related data must be handled in compliance with data privacy regulations. Registration of orally made reports has even stricter requirements.

4. Organisations and companies must protect the whistleblower (Article 19)

Finally, the Directive sets requirements regarding **protective measures** concerning the reporter and other individuals involved in the report. In order to be entitled to such protective measures, the reporter must have had reasonable grounds to believe that the disclosure of the information was necessary for revealing a breach (of Union law). The Directive includes a prohibition of retaliation and imposes an obligation to implement safeguards against it. These measures are extensive and will significantly restrict organisations' actions towards a whistleblower.

Organizations and their management need to be aware of such restrictions and make sure the requirements are not (accidently) breached.

A recent court case in France illustrates how the protection for whistleblower works in practice. Although this case was made on the basis of the former applicable law in France, it is still relevant to illustrate the concrete application of the provisions of the Whistleblower Directive. An employee of Thales, a French multinational specialised in the manufacturing of equipment for the aerospace, defense and security, alerts her hierarchy about facts that could potentially qualify as corruption in the company. The ethic committee, in charge of this alert, concludes that the facts cannot qualify as corruption. A few weeks later, the employee is fired. She hence decides to bring the case to court. The appeal court considered that the employee did not bring the evidence that her dismissal was unequivocally linked to her alert and the retaliation against her after her alert was not established. The appeal court concluded that the protective status for whistleblower established by the implementation law of the Whistleblower Directive had not been breached in that case. The 'Cour de Cassation' (highest court in France of the judicial order) disagreed with the appeal court and decided that, according to the implementation law of the Whistleblower Directive, **it is up to the employer to prove that the dismissal of an employee, who alerted potential facts of corruption and who benefits from the protective status for whistleblowers, is not linked to the employee's alert.** The High Court also considers that the qualification of the cause of the dismissal can be lawfully brought before a court ruling in emergency (Cass., Soc., 1 February 2023, Mme E against Thales, pourvoi n°

Penalties (Article 23)

It is up to the Member States to provide for penalties applicable to a natural or legal person. They must be “effective, proportionate and dissuasive”.

More information

Directive (EU) 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937

Download the Commission Factsheet on the EU Whistleblower Directive: https://commission.europa.eu/system/files/2018-04/placeholder_11.pdf

EU Whistleblowing Monitor: https://www.whistleblowingmonitor.eu

To check out the full list of the concerned areas of EU law: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3442

Cass., Soc., 1 February 2023, Mme E against Thales, pourvoi n° R21-24.271: https://www.courdecassation.fr/decision/63da1185b78bc005de6ccd13