EU whistleblowing rules to change in favor of whistleblowers

Alja Poler De Zwart

Abstract

Purpose – *To describe the new EU Whistleblowing Directive and its implications.*

Design/methodology/approach – *Describes organizations to which the Directive applies, the scope of reportable whistleblowing concerns, whistleblowers' reporting channels and mechanisms, whistleblower protections, how organizations should respond to whistleblower reports and how organizations should prepare for the new rules.*

Findings – *The new Directive will require Member States to create rules for organizations with more than 50 workers, will mandate such organizations to implement whistleblowing hotlines for reporting a broad range of EU law violations, and will contain minimum standards on how to respond to and handle any concerns raised by whistleblowers.*

Practical implications – *Organizations in the EU can and should start taking initial steps to prepare for the new rules as soon as possible. There will likely be some differences among whistleblower rules in individual EU Member States.*

Originality/value – *Practical guidance from experienced corporate, technology, media, telecommunications and compliance lawyer.*

Keywords *European Union (EU), Whistleblowing Directive, Whistleblowing reporting channels and mechanisms, Reportable whistleblowing concerns, Whistleblower protections, Retaliation*

Paper type *Technical paper*

Alja Poler De Zwart (apolerdezwart@mofo.com) is a partner at Morrison & Foerster (International) LLP, Brussels, Belgium.

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 (The "Whistleblowing Directive") came into force on December 16, 2019. The new Whistleblowing Directive requires the Member States to create rules for organizations with more than 50 workers and mandates such organizations to implement whistleblowing hotlines for reporting a broad range of EU law violations. For that purpose, the Whistleblowing Directive contains minimum standards on how to respond to and handle any concerns raised by whistleblowers.

The Member States need to implement the Whistleblowing Directive into local law over the course of the next year and a half:

1. Organizations with 250 or more workers will need to comply with the new rules by December 17, 2021; and
2. Organizations with 50 to 249 workers will have an additional two years to comply with a deadline of December 17, 2023.

National implementation inevitably means that there will be no full harmonization, so the whistleblowing rules in the EU will likely differ in the individual EU Member States. This will, to a certain extent, mean that multinational organizations with operations in various EU Member States will need to take local differences into account when setting up their whistleblowing hotlines.

In-scope organizations

Organizations with more than 50 workers will have to set up whistleblowing reporting channels, which is a change compared to the current situation, where the majority of Member States do not require the establishment of whistleblowing hotlines.

The concept of a "worker" in the EU is broad. According to established EU jurisprudence, "workers" are individuals who, for a certain period of time, perform services for and under the direction of another individual, in return for which they receive remuneration. This includes regular employees and workers in non-standard employment relationships, such as part-time workers, trainees/interns, and fixed-term contract workers.

Consequently, organizations whose numbers of workers fluctuate around the 50 mark might have difficulties determining whether they fall under the Whistleblowing Directive's scope. If an organization is not certain whether it hits the 50 mark, or its numbers fluctuate around the 50 mark, it might be better to set up the channels anyway.

The Whistleblowing Directive also "*encourages*" organizations in private sectors with fewer than 50 workers to establish whistleblowing channels. If a Member State chooses to do so, it can impose less prescriptive requirements than the ones that are currently described in the Whistleblowing Directive, provided that such requirements guarantee confidentiality and diligent follow-up. This is something to keep and mind when monitoring the EU Member States' implementation of the Whistleblowing Directive. If such "encouragement" is included in the upcoming local implementing laws, organizations with less than 50 workers should take a closer look to identify any potential obligations.

Clarifications are needed

The Whistleblowing Directive does not provide clarity on whether the 50 workers need to be physically located in the EU. The EU Member States' implementing laws will hopefully provide additional details on this point. A reasonable interpretation is that any legal entity established in the EU that employs more than 50 workers will need to comply with the Whistleblowing Directive, no matter if such workers are located in or outside the EU.

The Whistleblowing Directive also does not address whether non-EU entities that employ more than 50 workers located in the EU will need to comply. However, European labor law, including regulations on worker protection and other employee protection provisions, applies to employees located in the EU, regardless of their employer's location. It is therefore highly likely that the entities will be subject to the Whistleblowing Directive.

The scope of reportable whistleblowing concerns

The allowed scope of reportable concerns is generally quite narrow under the current rules, and varies according to EU Member State. The Whistleblowing Directive harmonizes the currently fragmented situation and allows for reporting that, at a minimum, covers a broad range of violations of EU law. Such violations may pertain to public procurement, financial services, products and markets, prevention of money laundering and terrorist financing, product safety, transport safety, protection of the environment, radiation protection and nuclear safety, food safety, animal health and welfare, public health, consumer protection, protection of privacy and personal data, and security of network and information systems. Violations affecting the financial interests of the EU, and violations relating to the internal market, including violations of EU competition law, state aid rules, and corporate tax law are also included in the reporting scope.

Member States may extend the scope of reportable concerns when they implement the Whistleblowing Directive into their national law, and the expectation is that some Member States might indeed take advantage of this option. This might be the case for The Netherlands, where the current House for Whistleblowers Act already requires organizations with at least

50 workers to allow for reporting of "*suspicious wrongdoing*" without limiting it to violations of EU law. This is an additional reason to carefully monitor the local implementation processes in the 27 EU Member States.

Internal vs external channels vs public disclosures

Whistleblowers should be encouraged to first use internal reporting channels and report to their own organizations, if such channels are made available and are reasonably expected to work. If the internal channels are not established, or are set up inappropriate way, whistleblowers may turn to external reporting channels that are to be established in all Member States.

External reporting channels are required to ensure that:

- There is appropriate follow-up on the reports received; and
- The follow-up occurs within a reasonable timeframe, to give feedback to whistleblowers who have not been able to settle their concerns through internal reporting channels.

Whistleblowers have the right to report their concerns directly to external authorities when:

1. Organizations have not set up internal channels, or internal channels are used but do not function properly (e.g., because the report was not dealt with diligently or within a reasonable timeframe or no appropriate action was taken despite the internal investigation confirming the existence of a breach); or
2. A whistleblower has valid reasons to believe that: (i) he/she would suffer retaliation or (ii) the competent authorities would be better suited to take effective action. The latter would, for example, be the case where: (a) the ultimate responsibility holder within the work-related context is involved in the breach; (b) there is a risk that the breach or related evidence could be concealed or destroyed; (c) the effectiveness of investigative actions by competent authorities might be jeopardized (e.g., in the case of cartel and other violations of competition rules); or (d) the breach requires urgent action (e.g., to safeguard the health and safety of persons or to protect the environment).

If the abovementioned internal and external channels do not address a whistleblower's concerns appropriately, then the whistleblower may make a public disclosure. This could be the case, for example, if the reported breach was not appropriately investigated, no appropriate remedial action was taken, there is a risk of retaliation, or there is a low prospect of the breach being effectively addressed due to the particular circumstances of the case (e.g. evidence could be concealed or destroyed, or an authority might be in collusion with the perpetrator of the breach or even involved in the breach).

Types of reporting mechanisms

Organizations will need to enable individuals:

- To report in writing and submit reports by post, by physical complaint box(es), or through an online platform (via the Internet or an Internet platform); and/or
- to report by using the telephone hotline or another voice messaging system.

Another new provision includes that, upon whistleblower's request, such channels should also enable reporting by means of physical meetings, within a reasonable timeframe.

Third party service providers may still be engaged to receive reports on behalf of the organization, provided that they offer appropriate guarantees for independence, confidentiality, data protection, and secrecy. The Whistleblowing Directive suggests the use of external reporting platform providers, external counsel, auditors, trade union representatives, or employee representatives.

Anonymous reporting

The Whistleblowing Directive does not affect the power of Member States to decide whether organizations and competent authorities are required to accept and follow up on anonymous reports. This issue is therefore left to the Member States to decide in their local implementation. The Whistleblowing Directive does note, however, that whistleblowers who report or publicly disclose information on violations of EU law anonymously, and are subsequently identified and suffer retaliation, will still qualify for the protections of the Whistleblowing Directive described below.

Whistleblower protections

Whistleblowers who have acquired information on violations of EU law in a "*work-based relationship*" are protected by the Whistleblowing Directive. The protections will be granted irrespective of whether the whistleblowers are EU citizens or third-country nationals, and irrespective of the nature of their activities, or whether they are paid. Organizations should take a note of this broad scope that includes:

1. Individuals having the status of workers (such as current and former (part- or full-time) employees and temporary workers);
2. Individuals who are not workers but who can play a key role in exposing violations of the EU law and may find themselves in a position of economic vulnerability in the context of their work-related activities, (such as self-employed individuals providing services, freelance workers, contractors, subcontractors, suppliers, shareholders, and persons employed by managerial bodies);
3. Job applicants or individuals seeking to provide services to an organization, who acquire relevant information during the recruitment process or another pre-contractual negotiation stage and could suffer retaliation (such as in the form of negative employment references, blacklisting, or business boycotting); and
4. Volunteers and (paid or unpaid) trainees.

Types of protections afforded to whistleblowers

Member States are required to prohibit any form of retaliation against whistleblowers and are required to set up a number of protective measures for the whistleblowers, which include:

1. *Advice:* Free access to comprehensive and independent information and advice on available procedures and remedies;
2. *Remedial measures:* Appropriate remedial measures against retaliation, such as:
    - Interim relief to halt ongoing workplace retaliation (such as threats or harassment), or prevention of dismissal pending resolution of any legal proceedings; or
    - Reversal of the burden of proof (meaning that organizations will need to prove that they have not retaliated against the whistleblower instead of the other way around);
3. *Protection from liability:* Whistleblowers will not incur any liability for making whistleblowing disclosures and will not be considered to have violated any restrictions on disclosure of information imposed by contract or law (such as gagging clauses);
4. *Protection in judicial proceedings:* Whistleblowers will be able to rely on the Whistleblowing Directive and its implementing laws for the purpose of their defense during legal proceedings; and

5. *Additional measures:* For example, financial assistance and psychological support, and possibly even provisions on personal liability and penalties for the perpetrators of retaliation.

Eligibility for protection

To apply the abovementioned protections, whistleblowers must have reasonable grounds to believe (in light of the circumstances and the information available to them at the time of reporting) that the reported concern is true. Organizations should note that the motives of the whistleblowers are therefore irrelevant in deciding whether they should receive protection.

Report handling

Organizations will need to consider the following when handling whistleblower reports:

1. Whistleblowers must be provided with sufficient information about the internal reporting process as well as the procedures to report externally to the competent authorities. Such information can be posted at a visible location accessible to all potential whistleblowers and on the website of the entity, and could also be included in courses and training seminars on ethics and integrity;
2. Reporting channels must be designed and operated in a secure manner that ensures confidentiality of the identity of everyone involved, including the:
    - whistleblower;
    - any facilitators (i.e., individuals who may assist the whistleblower in the reporting process) as well as; and
    - third parties and implicated individuals mentioned in the report.
3. Organizations must designate individuals or departments to investigate reports independently who are impartial and free from conflicts of interest (e.g., dual function held by a company officer well placed to report directly to the organizational 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);
4. Organizations must ensure diligent investigation of the reported concerns;
5. Organizations may ask for further information during the course of the investigation, but the whistleblower will not be under any obligation to provide the information;
6. Organizations are required to acknowledge receipt of a report within seven days of that receipt; and
7. Organizations must provide feedback to the whistleblower within three months from the acknowledgment of receipt of a report or, if no acknowledgement is provided, three months from the expiry of the seven-day period after the report is made. The feedback should include the action envisaged or taken following the report, and the grounds for the choice of that action. The whistleblower does not have to receive this feedback if providing it could prejudice the investigation or affect the rights of the implicated individuals. When the appropriate action still needs to be determined, the whistleblower must also be informed accordingly. In all cases, the whistleblower must be informed of the investigation's progress and outcome.

Organizations should start preparing

Considering that the minimum standards are already set by the Whistleblowing Directive, organizations should not wait until the Member States' implementing laws are adopted.

Organizations can and should start taking initial steps to prepare for the new rules as soon as possible. When the compliance projects should start will likely depend on each organization's state of compliance with the current whistleblowing rules.

It is advisable that organizations without whistleblowing hotlines should start their compliance projects sooner rather than later. Such organizations will have a lot more work on their hands because they basically need to start setting up the hotlines from scratch. The process is usually not as simple as it looks, and it often starts with due diligence and engagement of a third-party hotline provider that can facilitate website and phone line reporting channels. So the sooner the organizations start preparing, the better.

Organizations that already have whistleblowing hotlines in place might find their compliance process a little easier to handle. This process will basically entail reviewing their existing hotlines and adjusting the relevant internal processes to what the Whistleblowing Directive requires. This may, for example, include the following:

1. The scope of concerns allowed to be reported for violations of EU law should be adjusted to the broader scope of the Whistleblowing Directive, unless the current scope in a specific Member State is already broader than the new provisions;
2. The whistleblowing hotlines that have been previously available only to an organization's current personnel, should be opened to other external individuals, such as former employees, job applicants, individuals seeking to provide services, subcontractors, suppliers, volunteers, trainees, and business partners;
3. The process of reporting should be adjusted to allow physical meetings with whistleblowers that can be set up within a reasonable timeframe;
4. Whistleblowing notices and policies should be updated to ensure that sufficient information is provided to potential whistleblowers about the internal reporting process, as well as external reporting procedures;
5. Organizations should ensure that a person or department designated to investigate whistleblowing reports can indeed do so in an independent and impartial manner, and free from conflicts of interest;
6. A process should be set up to acknowledge receipt of a report, unless the whistleblower explicitly requests otherwise, and provide feedback within the timelines specified in the Whistleblowing Directive;
7. The entire process should contain safeguards to ensure that whistleblowers are not pressured at any point to provide additional information when requested by the designated investigators. This may include instructing and training the investigators how to ask for such input to ensure maximum response and to know when to refrain from further actions if the whistleblower does not want to cooperate. Detailed internal investigation protocols that provide uniform and clear instructions on what investigators may and may not do are, as always, highly recommended;
8. Considering the possibility of whistleblowers reporting their concerns to external channels, effective and independent processes could be highly beneficial for organizations so that whistleblowers can complain to the organization (e.g., about not being taken seriously or being subject of retaliation) instead of going to authorities or the media;
9. As always, organizations should search for what else they can do to make individuals feel comfortable and safe when making internal reports. For example, organizations should consider ensuring that reporting channels are available 24/7, are simple and easy to use, offer anonymity protections (where allowed by the relevant Member State), are available in local languages, provide transparent explanatory information

and simple instructions, and are accompanied by an effective internal communication and investigation strategy.

10. Organizations should consider providing additional training and making it very clear that retaliation is absolutely prohibited. It should be stressed that anybody disregarding this prohibition in any way, shape or form will be subject to disciplinary measures, which could even include termination of employment; and

11. Last but not least, organizations are advised to monitor the Member States' local implementation to identify specific local requirements and adjust their hotlines accordingly.

Corresponding author

Alja Poler De Zwart can be contacted at: apolerdezwart@mofo.com