EU Whistleblower Directive: Key provisions, SOX comparison and Actions for business

June 2022

Por Antonio Carino | Pilar Menor | Brian S. Kaplan

Recent scandals such as the Luxembourg Leaks financial scandal and the Panama Papers have highlighted the important role that whistleblowers can play in exposing breaches of EU law. In particular, the workplace is often central to the identification of wrongdoing since individuals who work for, or have work-related contact with, an organization are often the first to learn of alleged misconduct in the organization. At the same time, fear of retaliation, and lack of legal protection against retaliation, may discourage them from reporting their concerns. Whistleblowing laws are currently implemented on a national basis across the EU and, in the majority of countries, protections can be fragmented, inconsistent, or even non-existent.

To address this situation, in 2019, the EU passed the Whistleblower Protection Directive, which had a deadline of 17 December 2021 for Member States to incorporate into their national laws. The Directive reflects the European Commission's view that Member States must have a legal and institutional framework to protect persons who, in the context of their industrial relations, draw attention to violations or to threats to the public interest or make information on them public. Subject to the provisions of local implementing legislation, public sector organizations and private sector businesses with 250 or more workers may need to comply from December 17, 2021. In respect of the requirements to set up internal reporting systems, a later implementation date of December 17, 2023, applies to private sector employers with 50 to 249 workers.

The new EU whistleblower laws herald a significant change in approach to whistleblowing in many EU countries, as well as significantly altering the compliance landscape for companies operating in the EU. Employers need to keep abreast of changes to ensure they have an approach that works for their business and achieves local compliance. In addition, multinationals that have long adhered to the US "gold standard" Sarbanes-Oxley Act may need to revisit their approach to ensure their programs satisfy the most extensive protections implemented by a Member State (while continuing to meet US requirements). While the EU framework will require many EU and multinational companies to make changes to their whistleblower programs, it also promises rewards. By ensuring that effective whistleblowing arrangements are in place, businesses have an opportunity to become aware of concerns at the earliest stages, helping to avoid or limit financial and reputational risks.

This article:

- outlines key provisions of the EU Directive;
- compares the EU Directive and the US Sarbanes-Oxley regime;
- identifies actions for employers to consider as they take stock of their programs and prepare for workplace whistleblowing compliance as new whistleblowing laws are implemented in each EU Member State; and
- considers practical elements of implementation and administration of an investigations program.

Whistleblower Protection Directive: Key Provisions

The Directive provides for minimum standards that must be adopted at national level. This means that EU Member States may choose to adopt provisions that strengthen the regime set out in the Directive but cannot adopt rules that do not meet the minimum standards of the Directive. These minimum standards are summarized below.

What can be reported?

The protection provided by the Directive will apply to individuals who report a breach of EU law in any of the following areas:

- public procurement
- financial services, products and markets, and prevention of money laundering and terrorist financing
- product safety and compliance
- transport safety
- protection of the environment
- radiation protection and nuclear safety
- food and feed safety, animal health and welfare
- public health
- consumer protection
- protection of privacy and personal data, and security of network and information systems
- breaches affecting the financial interests of the EU
- breaches relating to the EU internal market

Note that the Directive permits Member States to extend their national provisions to cover areas beyond those listed above, with a view to promoting a comprehensive and coherent whistleblower protection framework at national level. It is expected that many Member States will take this approach in their implementing legislation.

Who is protected?

The Directive applies to individuals working in the private or public sector who acquire information on suspected breaches in a work-related context. This definition specifically includes current and former:

- workers – this is a wide definition that includes not only employees but any individual who performs services for and under the direction of another person, in return for remuneration. Protection will therefore cover workers in non-standard employment relationships, including fixed-term workers, agency workers and other atypical relationships
- self-employed individuals, including freelance workers, contractors and subcontractors
- shareholders
- members of an undertaking's administrative, management or supervisory body
- volunteers
- trainees (paid or unpaid)
- those working under the supervision/direction of contractors, sub-contractors and suppliers
- new recruits who have not yet commenced work
- facilitators (someone who assists a person in the reporting process in a work-related context)
- third persons connected with a reporting person who could suffer work-related retaliation (eg colleagues or relatives)
- legal entities that the reporting person is connected to in a work-related context

What protection is provided?

An individual who meets the conditions for protection under the Directive is safeguarded from any form of retaliation and from threats of or attempt at retaliation. Member States must implement necessary measures to ensure this protection, including:

- It must be assumed that there has been retaliation and, in court proceedings, the burden of proof is on the organization to show that it has not retaliated. Where there is an allegation of retaliation for making a report, it is for the person that has taken the detrimental measures to prove that this was, in fact, based on justified grounds.
- Effective remedies must be available, including the possibility of interim relief, as well as remedies and full compensation for any damage suffered by a person who makes a report.
- Penalties for those that hinder reporting or retaliate against, disclose the identity of or bring vexatious proceedings against someone who has made a report must be effective, proportionate and dissuasive.

- The rights of someone who makes a report and the remedies available to them cannot be waived or limited by any form of agreement.

The Directive defines retaliation broadly to include:

- suspension, lay-off, dismissal or equivalent measures
- demotion or withholding of promotion
- transfer of duties, change of location of place of work, reduction in wages or change in working hours
- withholding of training
- a negative performance assessment or employment reference
- imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty
- coercion, intimidation, harassment or ostracism
- discrimination, disadvantageous or unfair treatment
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that they would be offered permanent employment
- failure to renew, or early termination of, a temporary employment contract
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry
- early termination or cancellation of a contract for goods or services
- cancellation of a license or permit
- psychiatric or medical referrals

Conditions for protection

To enjoy protection under the Directive the reporting person must:

- report either internally (within their employer’s organization) or externally (to a competent authority) or make a public disclosure (place information in the public domain); and
- have reasonable grounds to believe, given the circumstances and the information available to them at the time of reporting, that the matters they report are true. This requirement is intended to safeguard against malicious, frivolous or abusive reports as it withholds protection from individuals who deliberately report wrong or misleading information. At the same time, the requirement ensures that protection is not lost where someone reports inaccurate information because of an honest mistake. The motives of the person in reporting are irrelevant in deciding whether they should receive protection.

Anonymous reports

The Directive leaves it open to individual Member States to decide whether businesses and competent authorities are required to accept and follow up on anonymous whistleblowing reports. Whichever approach a Member State takes, however, an individual who makes an anonymous report must be given the protection of the Directive if they are subsequently identified and suffer retaliation.

Internal reporting

- Member States are to encourage internal, rather than external, reporting where a breach can be effectively addressed internally and where the individual reporting does not feel at risk of retaliation.
- Businesses, including private sector employers with 50 or more workers, must establish channels and procedures for internal reporting and for follow-up after consultation and agreement with social partners where required by national law. Note that for private sector employers with 50 to 249 workers the requirement to set up internal reporting systems does not come into effect until December 17, 2023.
- Reporting channels and procedures, which can be operated internally or provided externally by a third party, must:
  - enable individuals who fall within the scope of the Directive (see above) to report information on breaches;
  - provide for reports to be made either in writing, orally or both. Oral reporting should be possible by telephone or voice messaging system or in a physical meeting when requested by the reporting person;
  - be secure and ensure the confidentiality of the reporting person and anyone mentioned in the report;
  - provide for acknowledgement of receipt of a report within seven days;

- designate an impartial person/department to diligently follow up on reports (including anonymous reports if provided for in national law). The designated person/department must maintain communication with the reporting person, ask for further information if necessary, and provide feedback to them;
- provide for feedback to be given within a reasonable timeframe – not exceeding three months from receipt of the report. Feedback must include information on action taken or envisaged as follow-up and the grounds for such follow-up; and
- provide information on procedures for reporting externally to competent authorities or EU entities.

- Records of every report received must be kept, but for no longer than is necessary and proportionate to comply with the Directive and other legal requirements

External reporting

- Under the Directive, an individual may make an external report whether or not they have first made an internal report.
- Member States must designate competent authorities to receive, follow up and give feedback on external reports. The Directive prescribes various requirements which Member States must implement in relation to reports to designated authorities. In particular, a designated authority must establish an independent and autonomous reporting channel which must, for example, provide for:
  - reports to be made either in writing, orally or both;
  - acknowledgement of receipt of a report within seven days in most circumstances;
  - confidentiality of the identity of the reporting person, with very limited exceptions;
  - reports to be diligently followed up and for feedback to be given within a reasonable timeframe – not exceeding three months or six months where this is justifiable;
  - the final outcome to be communicated to the reporting person; and
  - reported information to be transmitted to other relevant EU bodies for further investigation in certain circumstances.

- Records of every report received must be kept, but for no longer than is necessary and proportionate to comply with the Directive and other legal requirements.

Public disclosure

An individual who makes a public disclosure of information will only be entitled to the protection of the Directive if:

- they first made a report internally or externally, but no appropriate action was taken in response to the report within the three/six month timeframe (see above); or
- they reasonably believe that:
  - the breach they are reporting is a matter where there is imminent or manifest danger to the public interest; or
  - if they reported externally there is a risk of retaliation or a low prospect of the breach being effectively addressed.

Scope for Member State-specific whistleblowing rules

As mentioned above, the Directive provides for minimum standards that must be adopted at national level but allows individual EU Members to adopt national whistleblower protection provisions that go beyond these standards and further strengthen the regime set out in the Directive. Thus, while an aim of the Directive is the harmonization of rules, it is possible that businesses will have to manage a patchwork of new rules depending upon the approach different countries adopt. In addition to the option for jurisdictions to “gold plate” the provisions of the Directive, there are also various aspects where the Directive permits countries to determine their own rules, including, for example:

- the application (if any) and scope of rules for organizations with fewer than 50 workers
- the scope of legal breaches which can be reported
- the approach to anonymous reporting
- penalties for retaliation

It is also not clear from the Directive how it will affect businesses with more than 50 employees but who are not all based in one EU Member State. This may be clarified in local implementing rules.

Comparison of EU Directive and the US Sarbanes-Oxley regime

For several years, there has been a significant global variation in the extent to which different countries have developed

national laws to provide for whistleblowing reporting channels, to ensure that reports are followed up, to protect whistleblowers against retaliation, and to strengthen accountability. For various reasons, including a cultural hostility towards whistleblowing, many European nations are among those countries that have not yet implemented rigorous whistleblowing protections. These variations can make it tricky for multinational employers, including those subject to the US Sarbanes-Oxley regime (SOX), to implement a global approach to whistleblowing and, in particular, to use whistleblowing hotlines that allow employees to report concerns confidentially and anonymously.

The arrival of the EU Whistleblower Protection Directive changes the global whistleblowing dynamic given that, in many respects, its provisions are wider than those that apply under SOX (see comparison table below). Although the Directive brings the EU in line with SOX by providing for the use of whistleblowing hotlines, one aspect where uncertainty remains is in relation to the handling of anonymous reports. SOX requires anonymous reports be accepted/addressed, but the decision as to whether or not this is required is left to each individual EU Member State. Global employers are urged to monitor this aspect of local country implementation and, more broadly, to consider whether other changes are required or desirable based on the scope of the Directive and any expanded Member State protections.

	EU Directive	SOX Regime
Which organizations must comply?	Legal entities in the public sector and legal entities in the private sector with 50 or more workers	• Publicly traded companies (ie companies with a class of securities registered under section 12 of the Securities Exchange Act of 1934) • Companies required to file reports under section 15(d) of the Securities Exchange Act of 1934 • Subsidiaries or affiliates whose financial information is included in the consolidated financial statements of such companies • Nationally recognized statistical rating organizations (as defined in 15 U.S.C. 78c(a)(62)) • Contractors, subcontractors, agents, officers, and employees of covered companies and nationally recognized statistical rating organizations A covered company's subsidiaries, contractors, subcontractors or agents may also be covered.
Types of wrongdoing that can be reported	Breaches of EU laws on: • public procurement • financial services, products and markets, and prevention of money laundering and terrorist financing • product safety and compliance • transport safety • protection of the environment • radiation protection and nuclear safety • food and feed safety, animal health and welfare • public health	Any conduct that the employee reasonably believes to be violation of: • mail, wire, bank, or securities fraud statutes; • any SEC rule or regulation; or • any provision of Federal law relating to fraud against shareholders.

	• consumer protection • protection of privacy and personal data, and security of network and information systems • breaches affecting the financial interests of the EU • breaches relating to the EU internal market	
Is an internal reporting system required?	Yes	Yes
Is an external reporting system required?	Yes. Under the Directive, an individual may make an external report whether or not they have first made an internal report.	Yes. Under SOX, an individual may report directly to the SEC whether or not they have made an internal report.
Do anonymous reports have to be accepted / addressed?	Each Member State to decide	Yes
Who is protected by the regime?	Reporting persons who acquire information on breaches in a work-related context including current and former: • workers • self-employed • volunteers • trainees • members of an undertaking's administrative, management or supervisory body • new recruits who have not yet commenced work • someone who assists a person in the reporting process in a work-related context • third persons connected with a reporting person who could suffer work-related retaliation (eg colleagues or relatives)	An individual presently or formerly working for a covered person, an individual applying to work for a covered person, or an individual whose employment could be affected by a covered person. See above for covered persons. In 2014, the US Supreme Court held that employees of private contractors and subcontractors of public companies are protected by the whistleblower provision set forth in 18 U.S.C. § 1514A of the Act subject to "various limiting principles" (eg the disclosures pertain to fraud perpetrated by a publicly traded company, as opposed to wrongdoing by a private contractor).
Is there protection against retaliation?	Yes	Yes

Does it apply to foreign subsidiaries or overseas branch offices?	Unclear	SOX covers subsidiaries or affiliates whose financial information is included in the consolidated financial statements of a company registered under Section 12 or required to file 15(d) reports. The Department Of Labor's Administrative Review Board has held that SOX's anti-retaliation provision does not apply extraterritorially. However, in some instances, conduct abroad may have a sufficient connection to the US to fall within SOX's protections.
Are financial incentives available?	Directive silent on the matter	Yes

*There are other federal, state and local statutes that prohibit private sector employers from retaliating against whistleblowers, many of which are industry or sector specific.

Recommended actions for employers

Implementation of the Directive across individual EU Member States has failed to meet the 17 December 2021 deadline in many cases and finalised legislation is awaited in the majority of countries. There are, nonetheless, various actions which businesses operating in the EU can take now to prepare for workplace whistleblowing compliance as local laws come into force. Recommended actions include:

- Monitoring progress of implementation in each EU country in which the company operates, taking particular note of those aspects where there is scope for differentiation (see above).
- Reviewing current whistleblowing arrangements or introducing new arrangements to ensure clear reporting channels are available. This will be the best way to avoid the risks associated with external reporting or public disclosure. Particular aspects of the Directive which may not form part of existing whistleblowing policies and procedures and should be factored in, include:
  - the obligation to provide information about procedures for reporting to external authorities;
  - the wide scope of matters on which reports can be made;
  - the extended scope of individuals who are permitted to report on breaches under the Directive (eg many current arrangements won't extend to former staff or to the self-employed, volunteers, trainees or recruits);
  - the specific timeframes for handling reports – seven days to acknowledge receipt and three months for providing feedback; and
  - the need for demonstrable follow-up to a report and feedback to the individual who has made the report.
- For businesses that have multiple hotlines for different purposes (eg employment issues, environmental health and safety), they should consider the benefits of having a central clearing house to make sure there is a full view of all the reports coming in, so the data points can be connected.
- A robust escalation policy so it is clear throughout the organization that regardless of how an issue is reported, it is escalated for transparency to the central clearing house.
- For businesses that provide or intend to provide a telephone/automated hotline as part of their whistleblowing procedures, ensuring these arrangements are configured to meet any particular jurisdictional requirements implemented by Member States. Local language considerations will also be important. In addition, the hotline provision will have to be expanded to the wider categories of individuals covered by the Directive – not just current employees.
- Change management exercise to map the current state and future state of investigational processes to ensure there is a direct cross walk of the policy, processes, work instructions and job aids such that these meet the new regulatory requirements. This should include a robust communication plan and training to drive this change.

- Preparing for the “reverse burden of proof” included in the Directive, which requires the employer to prove that any alleged retaliatory actions were based on justified grounds and not retaliatory.
- In addition to ensuring that all whistleblowing reports are diligently investigated and responded to by individuals who have been fully trained for the role, businesses should also ensure continued monitoring of, and record keeping as regards relationships with individuals who have made reports even after their matter is closed. This will enable a business to ensure there is no retaliation or that any adverse action subsequently taken is justifiable on legitimate grounds.

Practical elements of implementation and administration of an investigations program

It will be difficult or impossible for a company to administer different processes based on the location of the reporter. For example, if a report is about activity in Portugal, but is reported by an American citizen that was seconded to the Portugal operation, which set of processes should be used? What if later an identical report is submitted by a Portuguese citizen. It would tie an organization up in knots to administer reports differently.

The more practical way to consider all of this is to put in place a process that meets the relative standard of the EU Directive as it currently stands. Use that same process on a worldwide basis as an overall strategy. If Denmark adopts a more rigorous standard, such as requiring acknowledgement of the report in five days instead of seven, then the company can evaluate if that is a best practice they want to adopt or instead that only under specific circumstances would they meet this higher standard.

By creating one system with minor caveats, there are downstream benefits, including that it is easier to keep metrics and spot deviations from processes.

In addition to the overall process, there is a critical privilege strategy that comes into play as you consider having to prove that no retaliation has occurred. Previously, the layers that had to be pierced by the government or a plaintiff were as follows:

- allegation (report)
- notes and response
- investigation report

At each stage, the business would assert privilege. The hope is that no party would get access to the investigations report. However, now the business needs to prove it did not retaliate. As a result, the business may have to share more, but still has elements of legal guidance that it will want to shield. Consequently, the new hierarchy is as follows:

- allegation
- notes and response
- standardized investigation report
- legal memorandum or guidance

Clients would be advised to have a standardized investigation report that they use to summarize all matters. This would be a two-six page templated report that captures the essential elements, but no more. For example, there may be eight pages of notes on an interview and a 20-page legal memorandum advising the company. The standardized report would leave out the legal guidance and may summarize the interview into a few critical bullet points.

The standardized report could be produced as necessary, particularly in defense of claims of retaliation. The legal memorandum would be held as privileged with the hope that it would not be necessary to produce it.

Return to Overview page

For a pdf of the full guide please click on the button below.

Access the full guide

AUTHORS

Antonio Carino
Socio
Milán | T: +39 02 806181
antonio.carino@dlapiper.com

Pilar Menor
Senior Partner
Madrid | T: +34 91 319 12 12
pilar.menor@dlapiper.com

Brian S. Kaplan
Socio
New Jersey (Short Hills) | T: +1 973 520 2550
New York | T: +1 212 335 4500
brian.kaplan@dlapiper.com