

RESPONDING TO THE EU WHISTLEBLOWING DIRECTIVE: SIX KEY ACTIONS YOU NEED TO TAKE NOW

Organisations and public bodies affected by the Directive will need to undertake a range of activities to comply with the new rules

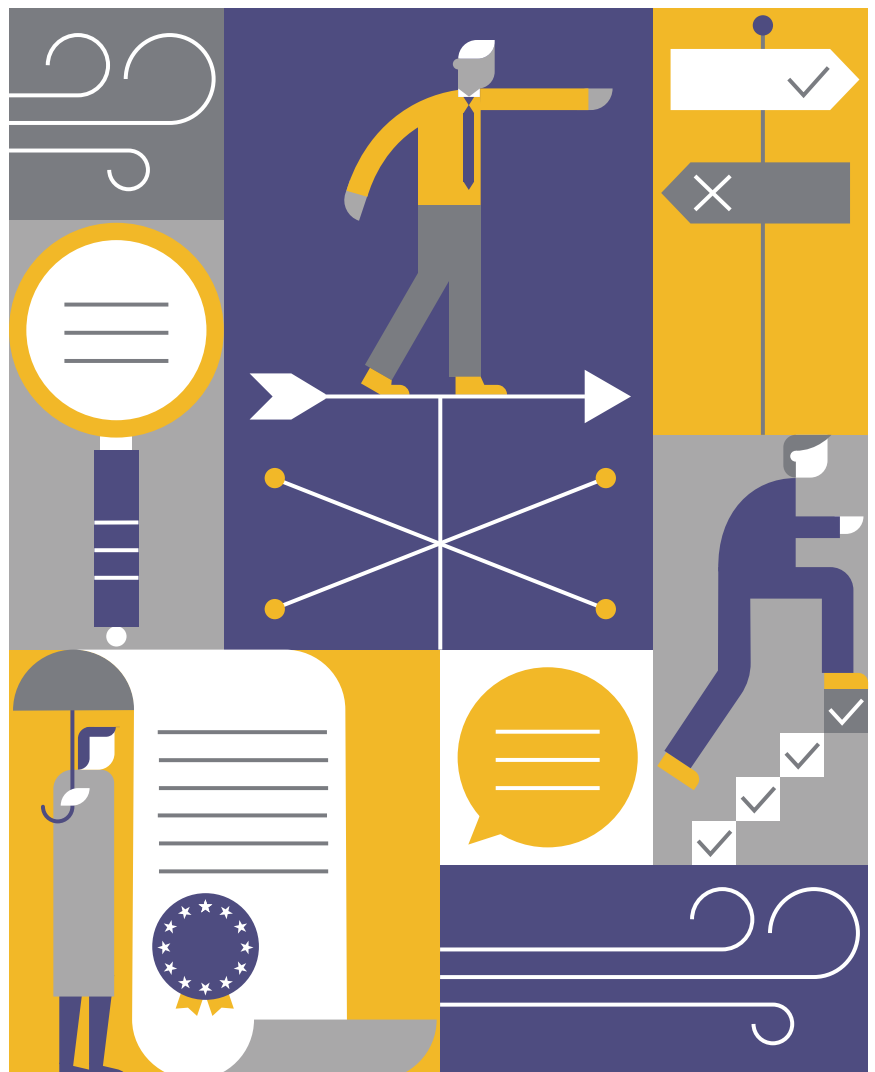
In October 2019, the European Council approved the *European Union's Directive for the protection of persons reporting on breaches of Union law* (or 'Whistleblower Protection Directive').

The Directive has been created in response to a series of scandals uncovered in recent years by whistleblowers, including both the Cambridge Analytica scandal and the Panama Papers, which highlighted the lack of protection for those who seek to expose corporate wrongdoing in the public interest.

A 2017 Special Eurobarometer on Corruption commissioned by the EU highlighted that fewer than one-in-five Europeans (18 per cent) would speak up about corruption if they witnessed it in the workplace and almost a third (29 per cent) believed that there is no protection for those that do expose wrongdoing.

The Directive is intended to change this. Following its formal adoption in October 2019, EU member states were given two years to implement it into national law. Organisations with 250-plus employees must comply with this legislation from 2021, and those with between 50 and 249 employees by the end of 2023.

Ahead of these deadlines, organisations need to fulfil these six key actions.



1 CREATE EFFECTIVE REPORTING CHANNELS AND PROCESSES

Central to the Directive is the obligation to create effective and efficient reporting channels in private and public sector organisations of over 50 employees, or municipalities of more than 10,000 inhabitants.

It will be up to each member state to decide whether anonymous reports should be accepted and followed up on, but the channels provided should enable people to report either in writing (through an online reporting platform, email or letter) or orally (via telephone hotline, voice messaging system or in person).

Line managers, HR and legal/compliance departments should be trained in how to handle reports in line with the new law and equipped to discuss employees' concerns. This should include understanding how to respond, who to inform and how to ensure confidentiality.

2 COMMUNICATE THE HIERARCHY OF REPORTING CHANNELS AND TRAIN EMPLOYEES

The Directive introduces a three-tier reporting system. Organisations



are expected to provide clear, easily accessible and transparent information about reporting channels in order to promote - and not deter - reporting.

In the first instance, employees should be encouraged to use internal channels to raise concerns, which should be kept confidential and responded to within three months.

The second tier enables employees to report concerns externally to "competent authorities" at EU or member state level. These cases must be dealt with inside three months (or within six months in justified cases).

The third tier enables whistleblowers to publicly air grievances through the media or other means. Such instances may involve an imminent danger to the public interest, a risk of retaliation or a failure to deal with concerns internally in the required timeframe.

3 UNDERSTAND WHO WILL BE PROTECTED

The Directive protects a broad range of individuals - essentially anyone working in the public or private sector who could acquire information about a breach in a work-related context. Those afforded protection therefore include (among others): employees, civil servants, the self-employed, volunteers, trainees, non-executive members and shareholders.

Protections also apply to those whose work-based relationship has yet to begin, such as through pre-contractual negotiations, or where it has ended.

Third parties or facilitators that assist those who speak up, for example colleagues or relatives who could be affected by a disclosure, are also protected.

4 BE AWARE OF THE WIDE SCOPE OF APPLICATION

The Directive's scope of application includes public procurement, financial services, the prevention of money laundering and terrorist financing, product safety, public health and the protection of privacy and

Employees at European-headquartered organisations use a range of reporting channels



Regional Whistleblowing Hotline Benchmark Report, NAVEX Global, 2019

personal data – in essence, any violation or potential violation of EU law that qualifies.

5 IMPLEMENT THE REQUIRED SUPPORT AND PROTECTION MEASURES

The Directive mandates organisations to implement and communicate the additional protective safeguards.

These ensure protection from retaliation such as dismissal, suspension, demotion, intimidation or other penalties, like being denied training or receiving poor evaluations.

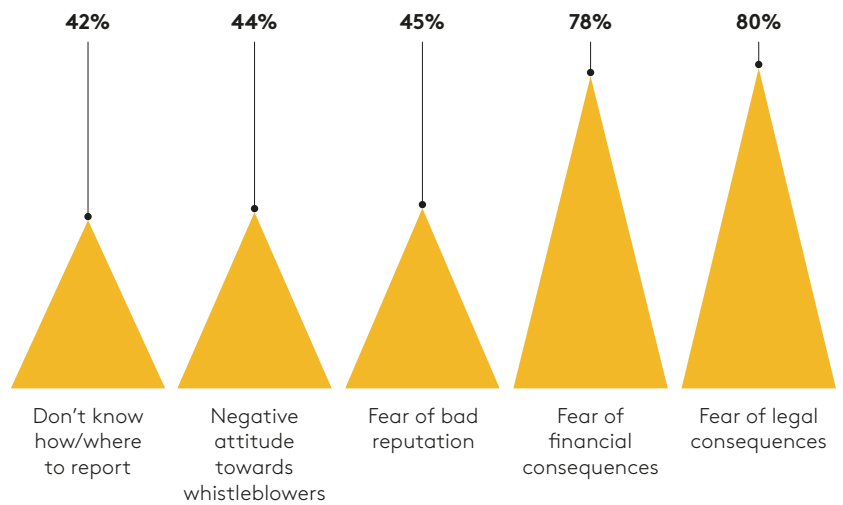
Protective measures also prevent the reporting person's identity being disclosed (without their consent) to anyone beyond authorised staff members who are competent to receive or follow up on reports.

In cases relating to detriment suffered by a reporter, the Directive presumes the detriment was made in retaliation to the report. This means the burden of proof in such cases will lie with organisations, rather than reporters themselves.

6 PUT PROCESSES IN PLACE TO MEET FEEDBACK OBLIGATIONS

With a window of three months, or six in exceptional cases, in which to respond and follow up on reports, organisations need to put effective management and response processes in place.

Why Europeans do not report wrongdoing



Open Public Consultation on Whistleblower Protection, European Commission, 2017

Organisations should clearly outline these policies and processes so that potential reporters know how their report will be handled, including what an investigation looks like, who will be conducting it and who will decide if wrongdoing has occurred.

Equally, organisations should provide information on what might happen to any individual found to have acted in breach of the rules and how they will be kept updated on developments.

For deeper analysis of the EU Directive, look out for NAVEX Global's upcoming *Whistleblowing Redefined* report.

NAVEX Global is the worldwide leader in integrated risk and compliance management software and services, and the world's largest provider of whistleblowing hotlines. Trusted by more than 14,500 customers, our solutions help organisations manage risk, address complex regulatory compliance requirements and foster an ethical, highly productive workplace culture. Find out more at www.navexglobal.com

NAVEX GLOBAL®

