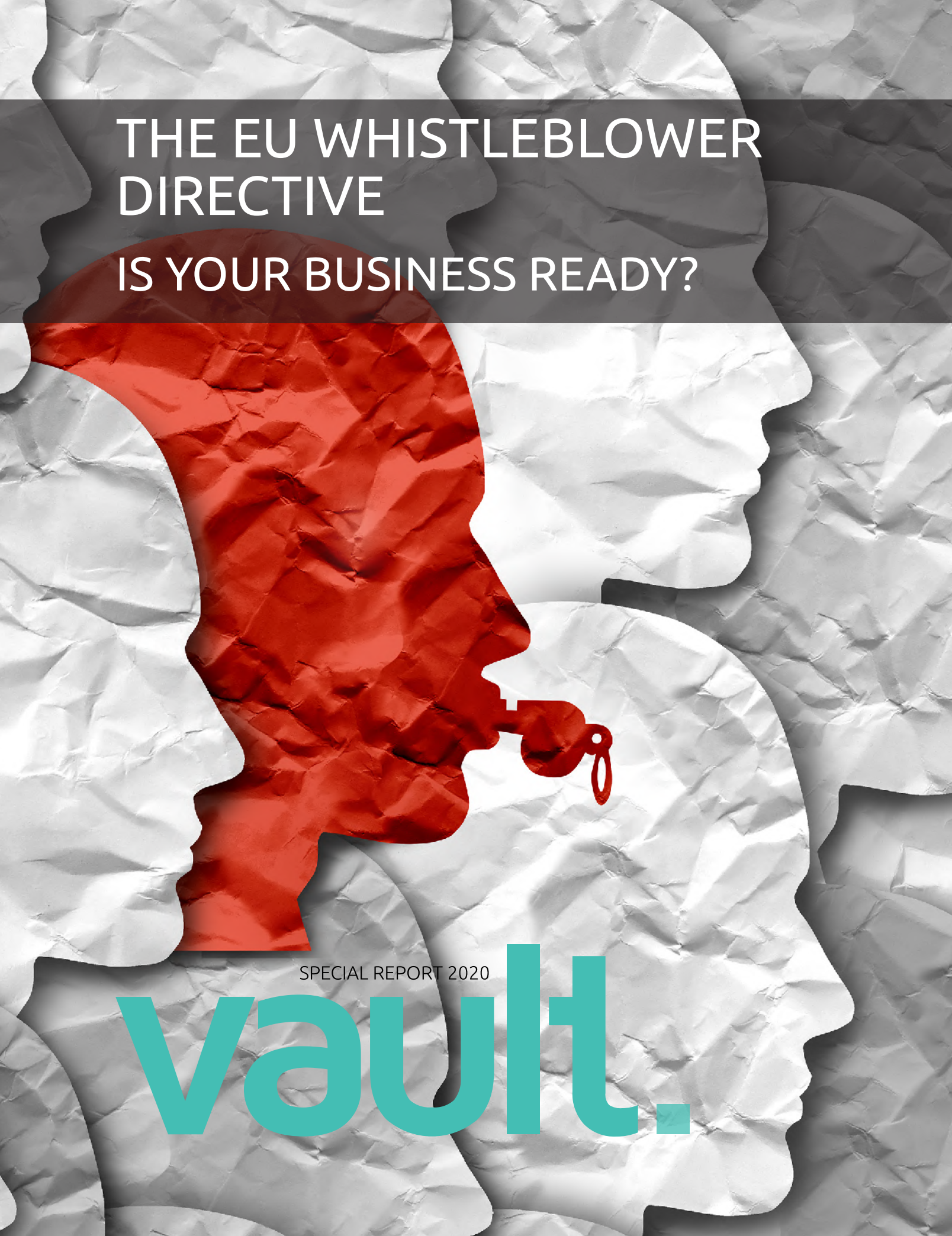
THE EU WHISTLEBLOWER DIRECTIVE

IS YOUR BUSINESS READY?



SPECIAL REPORT 2020

vault.

THE EU WHISTLEBLOWER DIRECTIVE WILL IMPACT EVERY EMPLOYER IN EUROPE

Every employer with more than 50 employees in the European Union will soon need to comply with the European Union's Directive for the protection of persons reporting on breaches of Union law, otherwise known as the EU Whistleblower Protection Directive.

The Directive was approved in October 2019 to grant greater protection for those who seek to expose corporate wrongdoing. EU member states were given two years to implement it into national law and adoption by enterprises will take a staggered approach. Organisations with more than 250 employees must comply with this legislation from December 2021, and those with between 50 and 249 employees by the end of 2023.

THE PROBLEM

Ahead of the release of the Directive, in 2017 the EU commissioned a Special Eurobarometer on Corruption. Although there is much variation from country to country, the report found on the whole that over two-thirds of Europeans think that corruption is widespread in their country and a similar percentage do not think corruption has not been tackled sufficiently by authorities or businesses.

However, as is the case with all forms of misconduct, the majority of Europeans who experience or witness corruption do not report it. Worryingly, over eight in ten respondents (81%) said that they did not report corruption that they experienced to anyone.

Of the challenges revealed in the report, the stand out one is that less than half of all Europeans would know where to report corruption. Furthermore, the main disincentives to reporting, aside from difficulties in proving their allegations, are the absence of consequences on the perpetrators and the lack of protection for those who report. Around one in three think reporting is pointless because those responsible won't be punished and a similar number are concerned that there is no protection for those reporting it. The Directive is intended to change this and establish an extended remit covering all breaches of Union Law, including health and safety and GDPR infractions. The Directive also covers a wide range of interpersonal misconduct with regards to retaliation for whistleblowing.

VAULT PLATFORM | THE EU WHISTLEBLOWER DIRECTIVE

WHAT IS A 'WHISTLEBLOWER'?

The term ‘whistleblower’ conjures up images of headline-grabbing figures such as Edward Snowden or Chelsea Manning, and has strong links with controversial characters such as Julian Assange. It’s also associated with large scale or high impact unethical behaviour such as the Volkswagen emissions scandal (Dieselgate) or perhaps the Enron scandal. But the truth is much more mundane and a cursory glance of a list of ‘famous whistleblowers’ reveals most of them to be everyday employees that decided to put their own neck on the line to expose some form of more localised misbehaviour they were witness to.

Moreover, the exposés are not always financial or political. Many have blown the whistle on several aspects of interpersonal misconduct as well, such as racial profiling in the United States Customs Service, or Ben Strickland’s allegations of sexual harassment within the US Coast Guard. The most recent and globally relevant example, however, is probably that of Li Wenliang, the eye specialist at Wuhan Central Hospital who raised the alarm on the COVID-19 virus in December 2019.

Not all incidents of whistleblowing are to external bodies. These just happen to be the ones we hear about because the whistleblowers went outside of their organisation. The term ‘whistleblowing’ is just as applicable to internal reports and should be the preferred channel for capturing and resolving ethical breaches. Unfortunately, it’s often when the internal mechanism falls short, is ineffective, or even not available, that whistleblowers often decide to take their concerns to an external party.

This is the main reason that as well as protecting the initial actions of those who ‘blow the whistle’, the Directive is also to safeguard against retaliation. Retaliation from the organisation or from peers or colleagues is a primary disincentive for anyone considering speaking up about behaviour that concerns them and is spotlighted time and again in the media. As is the case with Li Wenliang, who was investigated by Chinese police for “false comments”, or the UK’s Reverend Keith Osmund-Smith, a chaplain with West Mercia Police who was suspended from duty in 2016 after passing information to the media about the Telford child sex abuse ring after escalation through internal channels failed.

"Internal whistleblowing report volume is associated with fewer and lower amounts of government fines and material lawsuits"

- University of Utah & George Washington University

Evidence on the Use and Efficacy of Internal Whistleblowing Systems, 2018

WHAT'S NEW? ESCALATION AND REPORTING CHANNELS

Under the Directive, a three-tier reporting structure is being introduced. While whistleblowers are encouraged to use internal channels first, there is no obligation to do so, and they will still qualify for protection when reporting internally and externally. While this means that whistleblowers fearing retaliation from internal sources can use an external channel without fear, it raises the risk for companies with ineffective or inefficient internal reporting mechanisms that whistleblowers will immediately opt for more public disclosure.

WHISTLEBLOWERS CAN REPORT CONCERNS THROUGH:

Internal reporting channels: facilitated by the organisation

External reporting channels: facilitated by the relevant national authorities or the appropriate EU institutions

Public reporting channels: such as going directly to the media, or a public forum such as Twitter

VAULT PLATFORM | THE EU WHISTLEBLOWER DIRECTIVE

OPTIMISING INTERNAL REPORTING

From both a business benefits and organisational culture perspective, having prospective whistleblowers use an internal reporting channel first is by far the most desirable approach. Not only does this minimise the risk of financial and reputational damage of an incident going public, it also strengthens trust between the employee and employer even to the point of encouraging more people to speak up before concerns boil over. This also sets an example that misbehaviour will not be tolerated and employees will report it, making potential corruption or ethical breaches less attractive to perpetrators.

However, implementing an effective internal reporting system is no checkbox solution and touches upon concerns raised in the EU corruption special report.

Many large enterprises, especially those that have been around for some time, will have implemented an hotline as a ‘tick box’ solution. As illustrated in the EU report more than half of respondents wouldn’t know where to report misconduct if they tried. One of the most telling recent examples of this kind of implementation is Lloyds of London, which was exposed in 2019 after its hotlines had been unavailable for 16 months because someone forgot to renew the telephone provider contract.

Another insight into how companies tick a compliance box by buying a hotline but not making it accessible comes from the hotline providers themselves, with many of the established players reporting a steady decrease in hotline usage, forcing them to rethink their offerings for a world that has moved on. The shift away from telephone hotlines was highlighted as far back as 2012 in the National Business Ethics Survey of Fortune 500 Companies, which revealed hotlines as the least popular channel (used only by 11% or reporters) among the small number of people that do go ahead and report misconduct.

With a multigenerational workforce that largely favours digital communications, the idea of telephoning a call centre somewhere to report misconduct might seem alien. It’s also inconvenient and unengaging, two significant modern trends that legacy reporting solutions have failed to address. Ultimately, hotlines are seen as outdated legacy offerings that really do little to solve a persistent problem and the public financial exposés post 2008, the interpersonal misconduct revelations of 2017, and employee activism of 2020 all support this.

"Hotline reporting channels aren’t enough"

- A leading whistleblower hotline provider

THE RISE IN EXTERNAL WHISTLEBLOWING

The frustration with and lack of effectiveness of internal reporting systems is considered to be the leading cause of whistleblowers opting for more public and external channels to raise their concerns.

The Future of Work survey, released by law firm Herbert Smith Freehills at the end of 2019, revealed that 80% of surveyed enterprises globally expect to see a rise in activism

among both employees and casual workers in the future. Around 40% think they will see a significant increase.

Social media will continue to play a key role as a tool for both coordinating and amplifying workforce activism. Some 95% of respondents to the law firm's survey said they expect to see an increase in their workforce making its voice heard through social media channels in the future.

But the risk isn't always from external exposure. If a void exists because the organisation failed to provide a mechanism, that void may be filled by the employees themselves, which in the case of companies that do eventually do the right thing, can even increase friction if the employee-owned tool has become established. Nike is a great example here. Amid concerns of sexual harassment within the company, a group of women quietly surveyed their colleagues in 2018 and found the concern was widespread. The survey findings eventually made their way to the CEO and prompted an exodus of senior executives.

The point is that with employees taking a grassroots approach, employers are losing control and visibility of reporting mechanisms, increasing the potential of reputational damage to the brand. The financial implications are significant, with the law firm suggesting employee activism could cost as much as 25% of an organization's global revenue per year.

But this is information companies can act on. In the research, 55% of enterprise respondents identified workforce actions as a risk to reputation, exceeded only by cyber threats, and global economic slowdown. Yet, in light of the current pandemic and ever-present threat of cyber attack, workforce action is the element organisations have the most and perhaps significant control over.

A failure to close the loop increased employees' belief that speaking up was futile by 30%

But if the organisation had closed the loop in the past, their employees spoke up 19% more frequently

- James Detert, Professor, UVA Darden School of Business

The wisdom of the crowd and strength in numbers are well understood psychological concepts and studies in organisational culture show that people are more likely to come forward if they see previous whistleblowers treated fairly, such as no retaliation and action taken.

One of the key challenges with incumbent anonymous reporting solutions is an inability to 'close the loop' - not follow up with the reporter - leading to a perception that no action was taken. In surveys of more than 3,500 employees in multiple companies, renowned organisational psychologist James Detert found that a failure to close the loop increased employees' belief that speaking up was futile by 30%. But if the organisation had closed the loop in the past, their employees spoke up 19% more frequently.

WHAT DO I NEED TO KNOW?

WHO NEEDS TO COMPLY?

In short, all legal entities with more than 50 employees operating within the EU member states are required to comply with the Directive. This includes European operations of organisations headquartered outside of the EU. The purpose of the Directive is "to enhance the enforcement of EU law and policies in specific areas by laying down common minimum standards providing for a high level of protection of persons reporting on breaches". At the time of the Directive's adoption, the EU warned that the majority of EU countries did not have effective laws in place, suggesting a significant liability for organisations across the EU Member States. In fact, the EU identified only 10 Member States with a 'comprehensive law' protecting whistleblowers: France, Hungary, Ireland, Italy, Lithuania, Malta, The Netherlands, Slovakia, Sweden and the UK. The Directive however, goes beyond these 'comprehensive' laws and will likely see adoption as countries seek to retain their pioneering position.

Legislation and provisions for employers includes reporting for all people having "Worker Status" plus: Self-employed, Trainees, Volunteers, Shareholders & NEDs; Former & Future employees (such as those who have gone through recruitment/pre-contract); and "Natural Persons" eg. Suppliers, Consultants, Freelancers, Contractors & Subcontractors.

Whistleblowers should be able to submit reports and these reports should be received and acted upon by a "most suitable" person, such as Compliance officer; Head of HR; Legal counsel; Chief Financial Officer (CFO) or other executive manager; or an appropriate external ombudsman.

The identity of the whistleblower must be kept confidential whether the report is submitted anonymously or not and all personal data, both that of the whistleblower and any accused persons, must be handled in accordance with the GDPR.

The company is obliged to confirm receipt of the report to the whistleblower within seven days. The whistleblower must be informed of any action taken within three months, as well as the ongoing status of the internal investigation and its outcome.

The internal reporting system must allow for a physical meeting to be requested and must outline external reporting procedures available to the reporter.

Companies that obstruct or attempt to obstruct the reporting of concerns will face penalties. Retaliatory measures against whistleblowers will also be punished, including a failure to keep the identity of the whistleblower confidential.

Organisations with more than 250 employees must comply with this legislation from December 2021, and those with between 50 and 249 employees by the end of 2023

WHAT BREACHES FALL UNDER THE REMIT OF THE EU DIRECTIVE?

- **Public Procurement Rules**
- **Financial Services Rules**
- **Product Safety Rules**
- **Transport Safety Rules**
- **Environmental Protection Rules**
- **Nuclear Safety Rules**
- **Food Safety Rules**
- **Animal Health & Welfare Rules**
- **Public Health Rules**
- **Consumer Protection Rules**
- **GDPR/Data Privacy Rules**
- **Breaches affecting the financial interest of the Union**
- **Breaches relating to the internal market**

It should be noted that this list is effectively extended under provisions for protection against retaliation.

WHAT COULD BE CONSIDERED 'RETALIATION' UNDER THE DIRECTIVE?

- **Suspension, lay-off, dismissal etc.**
- **Demotion or withholding of promotion**
- **Transfer of duties**
- **Negative performance assessment**
- **Disciplinary measures, reprimands, financial penalty**
- **Coercion**
- **Intimidation**
- **Harassment**
- **Discrimination**
- **Failure to convert temporary/fixed term employment or to renew**

Although not mandatory, forward-thinking employers are ensuring their whistleblowing solution is also able to capture incidents of retaliation. This makes reporting, attribution, and resolution much easier, as well as reducing the number of separate tools performing similar tasks

THE DEADLINE IS LOOMING

Every employer with more than 50 employees in the European Union will soon need to comply with the **European Union's Directive for the protection of persons reporting on breaches of Union law**, otherwise known as the **EU Whistleblower Protection Directive**.

Organisations with more than 250 employees must comply with this legislation from December 2021, and those with between 50 and 249 employees by the end of 2023.

With the safeguards set out in the Directive, the EU is signaling to whistleblowers that they have nothing to fear while encouraging workers to report on company wrongdoing.

AHEAD OF THE DEADLINE YOU NEED TO:

- **Communicate the impact of the Directive to essential stakeholders,** including new responsibilities
- **Communicate the impact of the Directive to all employees,** identifying who is protected and what is covered
- **Communicate the hierarchy of reporting channels** and why/when they should be used
- **Implement tools and processes to:**
    - Capture reports
    - Confirm receipt of reports and provide updates
    - Allow for further communication and feedback between reporter and investigator
    - Allow for resolution update
- **Ensure the tools and processes retain confidentiality** of identities and are compliant with GDPR
- **Update policies to reflect new implications**
- **Make sure all the above information and policies are easily accessible**
- **Communicate the whistleblowing process and 'how to' to all employees** and have a campaign plan to frequently disseminate this information

ARE YOU COMPLIANT WITH THE EU WHISTLEBLOWER DIRECTIVE?