onetrust

How to build a speak-up culture

Your step-by-step guide to raising hotline awareness and improving reporting rates

E-BOOK | JANUARY 2023

Table of Contents

Introduction 03

Step 1: Conduct a listening exercise 04

Step 2: Raise awareness 05

Step 3: Address 'fear of the unknown' 07

Step 4: Address fear of retaliation 08

Step 5: Address cultural barriers 09

Step 6: Ensure employee confidence 10

Introduction

First, let's consider why a healthy speak-up reporting volume is important. The existence of a strong speak-up culture is widely accepted as fundamental to any ethics and compliance program. In addition to being legally required for many organizations, it is accepted as a key component of delivering a transparent culture with a strong sense of organizational justice and accountability. A recent study clearly identified the correlation between whistleblower report volume and business health.

What can you do to raise the number of reports you receive and ultimately build a stronger speak-up culture across your organization? It all depends on what is at the root of the problem. Common causes for suppressed reporting include:

- Lack of awareness that a hotline exists and why

- Fear of retaliation

- Reluctance to "tattle-tale" or "snitch" on colleagues

- Skepticism that a report will lead to change

So, what can you do to counteract these factors? In this eBook, we will explore six practical initiatives that you can implement today to increase hotline awareness and reporting.

Step 1: Conduct a listening exercise

Use simple analytics to identify where reports are coming from — and not coming from. It is possible that your problem is companywide, but it is more likely that you have pockets of silence. Several of our customers have used their analytics to find those areas where the speak-up volume is lower (using internal benchmarking).

Sometimes managers and supervisors will — wantonly or misguidedly — say things such as "Don't contact the hotline, we deal with any issues ourselves." If the analytics show low or no reports from certain countries, regions, divisions or plants, then use the analytics as an alert to investigate, understand and re-double communications. It may be that there are genuinely no issues to report, but it could be that reports are being suppressed, for a host of reasons.

You can also compare your reporting rates to other organizations' experience using a benchmarking application (external benchmarking). This will show you if the speak-up volume you are experiencing in certain countries or working environments is in line with societal trends, or if you have a unique internal challenge. It is important to understand where you have opportunities to improve the speak-up rate

before you dive into understanding why you have these challenges.

Through one-on-one interviews, workshops, surveys, and compliance program data, try to hone in on the exact reasons people are not speaking up through your hotline: Do they know it exists, is it readily available to them, do they fear repercussions, do they trust the anonymity of the service, do they trust the organization to take them seriously and investigate and act, do they believe that raising a concern is the right thing to do?

Key tools for success:

- Internal benchmarking
- External benchmarking
- Interviews, workshops, and surveys

Step 2: Raise awareness

With your team, brainstorm some ways to creatively make employees aware of your whistleblowing hotline. Here are some of the successful awareness campaigns our customers have implemented when they launch their OneTrust Speak-Up Program:

Make your hotline approachable. Give it a brand. For example, "Talk to Peggy" or "Ask Veronica." This humanizes the hotline, gives it an approachable face, and reduces the fear of communicating with a nameless agency (see Step 4: Address fear of the unknown).

Hang posters around the office (most commonly in bathroom stalls, as they are private), with tear off phone strips. Tear a couple of the numbers off, so people perceive that their colleagues are engaging.

Produce a credit-card-sized reference for people about the hotline (analysis shows that the resulting retention and awareness rates are very high, for a modest investment).

Include hotline details on employee passcards, identity cards and the like. Lanyards, pay slips, stickers inside company vehicle windscreens/ windshields are further examples of reminders that will be seen regularly, and are inexpensive.

Tailor your awareness program to your audience. Example: for manufacturing or factory workers, put the hotline message on a lens cloth — something that they will use several times each day to clean their safety glasses.

Some statutory documents will often need to be posted to employees at home; include hotline information in those types of periodic communication, where their surroundings will likely mean that they are more relaxed about reading it.

Create a digital presence where you can promote your ethics brand and host information on hotline and retaliation policies (e.g., OneTrust's Interactive Code of Conduct).

Send periodic and regular emails promoting the ethics program. Highlight specific areas of ethics and compliance in each email so they are different and interesting.

Supporting phrases such as "don't be a bystander" and "if it concerns you, it concerns us" can prove to be very compelling and, again, deliver valuable improvements in reporting levels.

Use stories to engage people. Ideally, tell anonymized stories of events that have happened in your organization: Investigation outcomes, examples of misconduct, etc., so people can grasp the tangible impact of ethics and compliance. This is a great way to highlight whistleblowers in a positive light (not by name) and express how they saved the organization from regulatory punishment, customer loss, waste, fraud etc....

Use "nudge" techniques to make the hotline message more compelling. Rather than saying "contact the hotline," use "contact the hotline – other people do" or "contact the hotline – your colleagues do." Embed videos in your ethics portal and link to them in your emails. These videos should include business leaders speaking to the individual's responsibility to report concerns. Change the tone from asking people to speak up to requiring them to speak up. This helps to mitigate their internal debate of whether they are doing the right thing. You remove the decision paralysis by requiring the action.

Step 2: Raise awareness (cont.)

With so many people working from home, think about how you can use technology to get your message in front of employees. We have seen some customers have IT insert an ethics message into the screensavers and wallpapers on employees' computers.

Use workshops: Arm team leaders with materials to host workshops with their teams. Have them discuss the types of concerns that should be raised to the hotline. Make it fun and engaging.

The EU Whistleblower Protection Directive (and some other laws) already require companies in their jurisdiction to support hotline reporting from a vast array of people, not just employees. For example, reports are accepted from people who went through the recruitment process but never joined the company, leavers, suppliers, vendors and even supporters of whistleblowers (such as family members) who have no direct relationship with the company. Consider how to address this type of third-party requirement including, say, a hotline link within supplier and vendor portals.

Recognize that COVID-19 and working from home may have affected hotline awareness and reporting metrics, particularly as people became increasingly concerned about keeping their jobs. Use return-to-work communications, reminders, and briefings (including Zoom/Teams) to raise hotline awareness.

Step 3: Address “fear of the unknown”

Making a hotline report can be a big step for people, and they will invariably be fearful of the unknown — such as “What will happen?” and “Who will know?” Every question like this can result in people deciding not to report, so addressing their “fear of the unknown” can be crucial. The following are a handful of ways that our customers have attempted to make their employees more familiar with their hotline and the reporting process.

Use reassuring imagery (of cats, dogs, people etc.) in hotline awareness campaigns to familiarize people with the hotline, whilst also subliminally reassuring and calming them.

When launching the hotline (and periodically thereafter), run a simple competition that invites everyone to make a simple first report — on canteen food, for example. Everyone who does so is entered into the competition with the possibility of a prize. In this way, people gain familiarity and even if they don’t participate, they still gain understanding and awareness for any future, serious reporting.

Explain the terminology: “Confidential” and “anonymous,” for example, can be confusing. Confusion can result in concern, which again leads to people deciding not to report.

Key tools for success:

- Employee awareness campaigns

- Hotline reporting competitions

Step 4: Address fear of retaliation

In all communications, emphasize the absolute protections of anonymity and confidentiality.

Promote the perception of organizational justice. People must believe that the company treats all people equally. Executive or high performers must be seen to be held to the same standards as everyone else. Tell stories (anonymized) about how high performers have been held accountable for transgressions.

Communicate the absolute nature of your antiretaliation policy. Share visibility into some of the checks and balances you monitor for retaliation.

In workshops, have local leaders reinforce the message that retaliation will not be tolerated.

Follow up with reporters regularly after their report to provide support (a.k.a. "report and support") and identify whether they have faced retaliation (some retaliation can be subtle, and undertaken over time).

- Use simple analytics to see what happened to their career, pay, shift allocation etc., post-report, and use this in the follow-up.
- Some retaliation occurs more than six months after the report, so reporter support is not a "one-and-done" activity.

Key tools for success:

- Workshops with local leaders
- Anti-retaliation follow up strategy

Step 5: Address cultural barriers to whistleblowing

(For example: "We do not do that here.")

Some cultures and countries have a history where informers were regarded as antisocial, collaborators with occupying forces, or similar. For example, citizens of many European countries developed strong perspectives on reporting in the wake of World War II. Citizens of these countries continue to have an aversion to whistleblowing. To overcome this, share messaging from team members and executives promoting the hotline. The message can be about protecting the company. It is not about the one or two people that are involved in the transgression; it is about the thousands of people whose livelihoods would be threatened if the company suffered a setback by the actions of the few bad apples.

You should also communicate examples of how people speak up, so that it is not seen as abnormal or isolated.

One example would be to share results of an employee survey, e.g., 90% of our employees said that if they saw something out of the ordinary, they would report it. Or share hotline metrics, e.g., we have 50 concerns raised through the hotline monthly.

Reinforce messaging about the purpose and values of the company. The hotline is here to protect that purpose.

Have local leaders use workshops to raise awareness on the importance of raising concerns. Give them tools like Giving Voice to Values for the teams to exercise and practice the behavior

Key tools for success:

- Teammate reinforcement
- Example sharing
- Giving voice to values

Step 6: Ensure employees know their concerns will be taken seriously

People often do not report concerns because they do not believe that their concern will be addressed. This can be mitigated by sharing stories in your monthly newsletter of how cases have been investigated and involved parties were held accountable.

Investigate cases efficiently and inform the reporter of progress and conclusion (at an appropriate level). This makes the reporter feel that their concern is being taken seriously and they will share this within the organization. Build a reputation for caring, efficiency, empathy, and confidentiality.

It can be worth testing and analyzing what happens after a report has been received, including the tone and perception of subsequent communications and interactions. These can make the difference between a “highly regarded” hotline and a “going-through-the-motions” hotline, with all the consequences for future reporting levels that will bring.

Annual (anonymized) compliance and ethics reports can play a key role here, with a hotline/discipline related subset published internally that shows reports are investigated and the actions taken up to and including dismissal/termination. Use the practices stated above in raising awareness, as they will reinforce the importance of reporting concerns.

Key tools for success:

- Workshops with local leaders

- Anti-retaliation follow up strategy

onetrust

As society redefines risk and opportunity, OneTrust empowers tomorrow's leaders to succeed through trust and impact with the Trust Intelligence Platform. The market-defining Trust Intelligence Platform from OneTrust connects privacy, GRC, ethics, and ESG teams, data, and processes, so all companies can collaborate seamlessly and put trust at the center of their operations and culture by unlocking their value and potential to thrive by doing what's good for people and the planet.

onetrust

The global regulations driving third-party due diligence

Key regulations to know for managing third-party risk

E-BOOK | APRIL 2023

Table of Contents

An evolving regulatory context for third-party due diligence 03

Preventing bribery and corruption 05

Complying with economic and trade sanctions 07

Protecting human rights across the supply chain 09

Combating money laundering and terrorism financing 11

Be informed about the regulations that impact your risk 13

An evolving regulatory context for third-party due diligence

The third-party risk management (TPRM) lifecycle is evolving quickly as a host of new regulatory drivers influence what responsibility companies have for their relationships with third parties. A robust third-party due diligence (TPDD) strategy, incorporating the latest regulatory drivers, will help your organization minimize risk, avoid hefty fines, and safeguard its reputation.

Let's begin by defining some key terms and then move on to a discussion of the changing regulatory environment for third-party risk management.

- **Bribery and corruption**
- **Sanctions**
- **Human rights**
- **Money laundering & terrorism financing**

An evolving regulatory context for third-party due diligence

What is third-party due diligence?

A **third party** is any outside entity or individual a company does business with — including suppliers, vendors, agents, partners, contractors, and distributors. Third parties may provide raw materials, finished products, or services to your organization or on its behalf.

Third-party risk management is the process of identifying, assessing, and mitigating risks associated with third parties. It's an important business discipline that helps you reduce the occurrence and impact of issues related to third parties. Companies rarely operate in isolation; instead, they're part of dynamic ecosystems of partners and service providers. But those relationships introduce complexity around ethics and compliance, as well as security, privacy, and environmental, social, and governance (ESG) risks. As a result, companies are adopting new strategies for managing third-party risks.

Third-party due diligence is any process taken to identify the specific risks a third party, or your relationship with them, may present. Third-party due diligence is just one stage of the third-party management lifecycle, which also includes intake, assessment, review, reporting, and monitoring. Third-party due diligence helps you make an informed decision about whether to engage with a particular third party, and if you choose to, how to best mitigate any risks identified.

Why does third-party due diligence matter?

Third parties can expose you to different kinds of risks. Some examples include:

- Violation of applicable laws resulting in significant fines, civil action, and/or criminal action, including imprisonment
- Damage to your company's reputation
- Violation of your company's standards and policies
- Financial loss or loss of new business opportunities

Third-party due diligence functions like a background check on your suppliers, vendors, distributors, and other third parties. Their actions can reflect negatively on your brand.

Changes in the regulatory environment are accelerating

Increasingly, regulators are holding businesses accountable for the conduct of third parties they do business with. A variety of regulations around the world now hold companies accountable for the actions of their business associates — and the changes in this regulatory environment have only been accelerating. But keeping track of all those regulations and their requirements can be challenging, as they frequently get updated or replaced by newer laws.

The scope of relevant regulations driving third-party due diligence is wide. In this eBook, we'll focus on four major categories: bribery and corruption, sanctions, human rights, and money laundering and terrorism financing. In each of the following sections, we'll explain the most essential regulations to be aware of today as you form your third-party due diligence strategy.

Preventing bribery and corruption

Global companies typically operate within a large network of partners, suppliers, vendors, and other third parties. Preventing bribery and corruption — not only internally but in their extended network — is critical for maintaining compliance. With enforcement penalties increasing and new laws coming into effect, organizations need a robust third-party due diligence program to prevent bribery and corruption. Some regulations in this category also limit penalties for companies that have effective internal compliance procedures in place.

Below are four major regulations on bribery and corruption for compliance teams to address:

- **US Foreign Corrupt Practices Act**
- **UK Bribery Act**
- **Brazil's Clean Company Act**
- **France's Sapin II**

US Foreign Corrupt Practices Act (FCPA)

The FCPA makes it unlawful for a US person or company to offer, pay, or promise to pay money or anything of value to any foreign official for the purpose of obtaining or retaining business. The FCPA applies to direct and indirect bribes by any officer, director, employee, or agent of a company or any stockholder acting on behalf of the company — including third parties acting on behalf, at the direction, or with the knowledge of the company.

The US Department of Justice (DOJ) expects organizations to implement controls in business relationships with third parties that act on their behalf in order to prevent bribery of foreign officials to gain a business advantage. The DOJ publishes detailed guidelines on how it evaluates corporate compliance programs. You can find this and other resources on the DOJ's website.

Preventing bribery and corruption

UK Bribery Act

The UK Bribery Act provides for the offenses of bribing another person, receiving a bribe, bribing a foreign public official, and the failure of commercial organizations to prevent bribery. As with the FCPA, the UK Bribery Act can hold an organization liable for bribes by any person associated with it — including people or entities that perform a service for or on behalf of the organization.

The act puts the onus on each commercial organization to prevent bribery by any persons associated with it by conducting due diligence. Due diligence includes appropriate procedures for bribery prevention, a top-level commitment, risk assessment, due diligence, communication, training, and monitoring and review. An organization will have a full defense if it can show that despite a particular case of bribery, it nevertheless had adequate procedures in place to prevent persons associated with it from bribing.

Brazil's Clean Company Act

Brazil's Anti-Corruption Law, known commonly as the Clean Company Act, targets corruption and bribery of local or foreign public officials by corporate entities doing business in Brazil.

The Clean Company Act holds companies liable for prohibited acts committed in their interest or for their benefit by employees as well as agents of the company. Organizations found to have breached the law can mitigate potential fines if they cooperate with Brazilian authorities and demonstrate that they have effective internal compliance procedures in place.

France's Sapin II law

The French Anti-Corruption Agency AFA Sapin II law requires companies to implement anti-corruption measures. The law applies to companies that operate in France with more than 500 employees and revenues of EUR 100 million.

Sapin II requires companies to create a code of conduct, engage in training, and create internal mechanisms for employees to report violations pertaining to bribery and corruption. Third-party risk management is built into the law, as Sapin II compels organizations to create a risk map to assess risks related to their clients, suppliers, and intermediaries.

Complying with economic and trade sanctions

Sanctions are commercial and financial penalties designed to advance foreign and security policy goals. They can include travel bans, asset freezes, arms embargoes, capital restraints, foreign aid reductions, and trade restrictions. Sanctions are a useful tool for managing international relations and foreign policy, and businesses must pay attention to how sanctions could affect how, and with whom, they do business to ensure they aren't doing business with individuals, entities, or countries that are subject to sanctions.

Regulators require businesses to determine whether their transactions involve sanctioned parties, so you need to include sanctions screening in your third-party due diligence in order to avoid violations.

Sanction regimes change quite frequently, so managing sanctions risk can be complex. The sanctions discussed here represent a non-exhaustive list — so bear in mind that other nations and sanctioning bodies may impose relevant sanctions in places where your company does business. In this guide, we'll discuss four key national and international sanctioning bodies:

- **US OFAC sanctions**
- **UK sanctions**
- **EU sanctions**
- **UN Security Council sanctions**

US OFAC sanctions

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury issues sanctions in support of US national security and foreign policy objectives. OFAC issues sanctions against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States.

OFAC sanctions include the Specially Designated Nationals (SDN) list, Consolidated Sanctions lists (non-SDN sanctions), Executive Orders, and others. OFAC regulations apply to US citizens, US incorporated entities and their foreign branches, and in some cases foreign subsidiaries owned by US companies. OFAC expects organizations to employ a risk-management framework to sanctions compliance.

UK sanctions

The UK's Sanctions and Anti-Money Laundering Act 2018, in support of furthering the UK's own objectives, enables sanctions related to compliance with UN and international obligations for the purposes of furthering prevention of terrorism, national and international peace and security, prevention of money laundering and terrorist financing, and combating threats to the integrity of the international financial system.

The UK Sanctions List provides details of current financial, immigration, trade, aircraft, shipping, and other sanctions. It is updated whenever the UK government makes, varies, or revokes sanctions. Legal entities within the UK or its territory should assess the risk profile of third parties and screen for relevant sanctions regimes.

Complying with economic and trade sanctions

EU sanctions

The European Union imposes sanctions to promote the objectives of the Common Foreign and Security Policy (CFSP), such as safeguarding EU values, interests, and security; supporting democracy, human rights, and international law; preserving peace; preventing conflicts; and strengthening international security.

EU sanctions apply to corporate entities constituted in a member state. EU companies should conduct due diligence by screening customers, suppliers, partners, and other third parties for sanctions risk.

UN Security Council sanctions

The UN Security Council may issue and enforce sanctions to maintain or restore international peace. UN Security Council measures include economic and trade sanctions, arms embargoes, travel bans, and financial or commodity restrictions.

UN sanctions apply to individuals and companies in all UN nation states. As with the US, UK, and EU sanctions, organizations in UN Member States should screen third parties to assess sanctions risk.

Protecting human rights across the supply chain

Responsible sourcing is an important part of any ethics and compliance program. Consumers, partners, and regulators all want to see organizations doing everything in their power to prevent human rights violations in their supply chains. Today, we're seeing a growing number of human rights, labor, and anti-modern slavery regulations implemented around the world. Some require companies to prevent human rights violations, and others, to report on the risks and their risk mitigation protocols. To meet these obligations, organizations must conduct third-party due diligence to assess third parties for potential risk of human rights violations.

No organization wants to be publicly exposed for human rights violations, so protecting your reputation necessitates thorough third-party due diligence across the supply chain. Here we'll look at six regulations related to human rights that could factor into your corporate third-party due diligence:

- **UK Modern Slavery Act**
- **Australia's Modern Slavery Act**
- **The California Transparency in Supply Chains Act**
- **Uyghur Forced Labor Prevention Act**
- **German Supply Chain Due Diligence Act**
- **France's Duty of Vigilance Law**

UK Modern Slavery Act (Section 54)

Section 54 of the UK Modern Slavery Act makes provisions about slavery, servitude, forced or compulsory labor, and human trafficking, as well as for the protection of victims. Section 54, Transparency in supply chains etc., covers supply chain transparency and mandates that commercial organizations prepare a slavery and human trafficking statement for each financial year of the organization.

The statement either (1) details the steps the organization has taken during the financial year to ensure that slavery and human trafficking is not taking place in any supply chains or part of its business or (2) expresses that the organization has taken no such steps. The statement should include a description of due diligence processes in relation to slavery and human trafficking, and it should be published on the company's website.

Australia's Modern Slavery Act

Australia's Modern Slavery Act 2018 requires in-scope entities to report on the risks of modern slavery in their operations and supply chains and actions taken to address those risks. The act applies to entities based, or operating, in Australia, which have an annual consolidated revenue of more than AUD 100 million. It requires such entities to report annually on the risks of modern slavery in their operations and supply chains, and the actions taken to address those risks.

The California Transparency in Supply Chains Act

The California Transparency in Supply Chains Act requires large retailers and manufacturers to provide consumers with information regarding their efforts to eradicate slavery and human trafficking from their supply chains. The act applies to retail sellers or manufacturers doing business in California with annual worldwide gross receipts in excess of USD 100 million.

Protecting human rights across the supply chain

Uyghur Forced Labor Prevention Act

The Uyghur Forced Labor Prevention Act (UFLPA) directs the US Forced Labor Enforcement Task Force to develop a strategy for supporting enforcement of the prohibition on the importation of goods into the United States manufactured wholly or in part with forced labor in the People's Republic of China, especially from the Xinjiang Uyghur Autonomous Region.

UFLPA applies unless the Commissioner of US Customs and Border Protection (CBP) determines that the importer of record has complied with specified conditions and, by clear and convincing evidence, that the goods, wares, articles, or merchandise were not produced using forced labor. The UFLPA encourages companies to exercise due diligence and closely examine their supply chains and conduct effective supply chain tracing and management measures such as supply chain mapping.

German Supply Chain Due Diligence Act

The German Supply Chain Due Diligence Act (SCDDA) addresses many aspects of supply chain ethics, including human rights, sustainability, and legal accountability throughout the third-party ecosystem. The law applies to enterprises that have their central administration, principal place of business, administrative headquarters, or statutory seat in Germany, and have at least 3,000 employees in Germany or abroad. (In 2024, the number drops to 1,000 employees.)

The SCDDA prohibits human rights violations such as child labor, forced labor and all forms of slavery, disregard of occupational safety and health obligations, and discriminatory treatment in employment, among other health, occupational, and environmental prohibitions. The SCDDA obligations apply across a company's supply chain, including all the steps necessary to produce its products and services. The SCDDA holds enterprises responsible for the actions of direct and indirect suppliers, specifically requiring them to conduct due diligence across their supply chains for human rights and environmental obligations.

France's Duty of Vigilance Law

France's Duty of Vigilance Law places a due diligence duty on large French companies pertaining to human rights and environmental issues, requiring them to publish an annual vigilance plan. The law applies to companies in France employing 5,000 or more employees in direct or indirect French subsidiaries or 10,000 or more employees globally.

The law explicitly requires French companies to conduct third-party due diligence. Specifically, the vigilance plan should include reasonable vigilance measures to identify risks and prevent serious violations of human rights, fundamental freedoms, and the health and safety of people and the environment resulting from the activities of the company and any other companies it controls directly or indirectly. This includes the activities of subcontractors or suppliers with whom the company maintains an established commercial relationship.

Combating money laundering and terrorism financing

Some organizations also face the risk of operators in their supply chain undertaking criminal activities such as fraud, money laundering, and the financing of terrorism. Therefore, you need to be aware of related laws and regulations and implement compliance measures related to the risk of financial crimes by your customers or third parties.

Money laundering is the process of concealing the origin of money obtained from criminal or illicit activities. Some regulations require companies to do due diligence on customers and third parties to monitor for potential money laundering.

The financing of terrorism involves soliciting, collecting, or providing funds that may be used to support terrorist acts or organizations.

In this guide, we'll cover four money laundering and terrorism financing regulations that could influence your third-party due diligence:

- **UK Proceeds of Crime Act**
- **UK Money Laundering, Terrorist Financing and Transfer of Funds Regulations**
- **EU Anti-Money Laundering Directives**
- **US Bank Secrecy Act and Patriot Act**

UK Proceeds of Crime Act

The Proceeds of Crime Act 2002 (POCA) addresses wide-ranging issues related to the "proceeds of crime," including provisions about money laundering in the UK. Under POCA, banks, other financial institutions, and firms in the regulated sector in the UK must put appropriate anti-money laundering (AML) controls in place to detect money laundering activities. These include customer due diligence and transaction monitoring measures, as well as a range of reporting requirements.

UK Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017

The UK Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 relate to the prevention of money laundering and terrorist financing.

These regulations apply specifically to the following persons and firms:

- Financial institutions, including banks, building societies, credit unions, and other deposit-taking institutions
- Money service businesses, such as currency exchange offices and money transmitters
- High-value dealers, such as dealers in precious metals, stones or watches, and art dealers
- Estate agents and letting agents
- Trust or company service providers, including formation agents and company directors
- Accountants and tax advisers
- Lawyers and notaries
- Casinos and online gambling operators

The regulations require firms to have policies and procedures for scrutinizing complex, large, or unusual transactions to ensure measures are taken to mitigate money laundering and terrorist financing risk.

Combating money laundering and terrorism financing

EU Anti-Money Laundering Directives

The European Union's Anti-Money Laundering Directives (AMLD) are designed to prevent the use of the EU's financial system for the purposes of money laundering and terrorist financing threats by ensuring that gatekeepers like banks and other obliged entities apply measures to prevent such crimes.

The directives require regulated entities to adopt a risk-based approach and evidence-based measures to customer due diligence. The AMLD regulations now address a range of crimes related to conventional money laundering, as well as cryptocurrencies, crypto exchanges, custodian wallet providers, and more.

US Bank Secrecy Act and Patriot Act

The Bank Secrecy Act fights money laundering in the United States. Focusing on due diligence obligations, it requires businesses to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax, and regulatory matters — such as reporting cash payments over $10,000 in trade or business. These documents are used by domestic and international law enforcement agencies to identify money laundering in furtherance of a criminal enterprise, terrorism, tax evasion or other unlawful activity.

The Patriot Act arms US law enforcement with tools to detect and prevent terrorism. The Patriot Act requires financial institutions in the US to perform due diligence on accounts established or maintained for foreign financial institutions, as well as private banking accounts established or maintained for non-US persons.

Be informed about the regulations that impact your risk

It's well understood that third parties can present significant risk to your organization. And as you can see, a wide variety of regulations influence how you conduct due diligence on third parties in your business ecosystem. Ethics and compliance teams often play a major role in screening against regulatory risk, reputational risk, and risk of third parties violating the company's policies. Staying informed about the latest regulations is critically important.

The regulations discussed in this eBook are a sampling of some of the predominant bribery and corruption, sanctions, human rights, and money laundering and terrorism laws around the world.

What we included here is far from an exhaustive list. But the requirements in any given area are generally similar, so you can establish one set of guidelines and processes across your organization to address a particular area of third-party risk.

No doubt — the regulatory drivers will continue to evolve, and third-party due diligence will become even more essential to protecting your brand from the risks third parties can impose.

Given the complexity of the regulatory drivers affecting your relationship with third parties, you may want to consider a third-party management solution to help you streamline compliance screening and management.

With OneTrust Third-Party Due Diligence, you can automate the third-party due diligence process — from initial screening to risk assessment and management to ongoing reporting and monitoring. The solution keeps third-party profiles in a centralized directory and uses data intelligence to alert you when a third party's risk profile changes.

Visit www.onetrust.com to learn more about how OneTrust Third-Party Due Diligence can protect you from third-party risk and help you build relationships with trustworthy partners in your business ecosystem.

onetrust

REQUEST A DEMO TODAY AT ONETRUST.COM

As society redefines risk and opportunity, OneTrust empowers tomorrow's leaders to succeed through trust and impact with the Trust Intelligence Platform. The market-defining Trust Intelligence Platform from OneTrust connects privacy, GRC, ethics, and ESG teams, data, and processes, so all companies can collaborate seamlessly and put trust at the center of their operations and culture by unlocking their value and potential to thrive by doing what's good for people and the planet.

onetrust

EU Whistleblower Protection Directive

E-BOOK | JUNE 2022

Table of Contents

SECTION 1
Introduction....04

SECTION 2
What the Directive requires....06

SECTION 3
Where the Directive applies and to whom....09

SECTION 4
Who is protected by the Directive....11

SECTION 5
What types of whistleblowing are protected by the Directive....13

SECTION 6
How whistleblowers can submit reports....15

SECTION 7
Retaliation and the reverse burden of proof....18

Table of Contents

SECTION 8
Anonymity and confidentiality 21

SECTION 9
Communications, awareness, and training 23

SECTION 10
Data Privacy and GDPR 26

SECTION 11
Finding a hotline vendor to help you comply 28

SECTION 12
About OneTrust 32

Introduction

European Parliament and the European Council adopted the Whistleblower Protection Directive on October 23, 2019. Before that date, whistleblower protection legislation in the EU – and beyond – was fragmented and inconsistent. The Directive's intention is to provide consistent protection for those who step forward and report breaches of EU law across all 27 Member States.

THE EU WHISTLEBLOWER PROTECTION DIRECTIVE TIMELINE

- April 2018 – EU Commission launches the proposal
- October 23, 2019 – Official adoption of Directive by EU Council
- June 24, 2021 – Denmark becomes the first to enshrine the Directive in local law
- September 29, 2021 – Sweden transposes the EU Whistlebler Directive into local law
- December 17, 2021 – Deadline for implementation by EU Member States and enforceable for organizations with 250+ employees
- December 17, 2023 – Enforceable for organizations with 50+ employees

"Companies should implement the unequivocal requirements of the Directive as soon as possible."

The Directive will greatly expand every dimension of whistleblowing and reporting – who can make a report, what can be reported, where issues can be reported and why. Not only that, but the Directive also expands the accountability that companies face when it comes to retaliation against whistleblowers. This presents some crucial, never-before-seen challenges to companies with a presence in the EU.

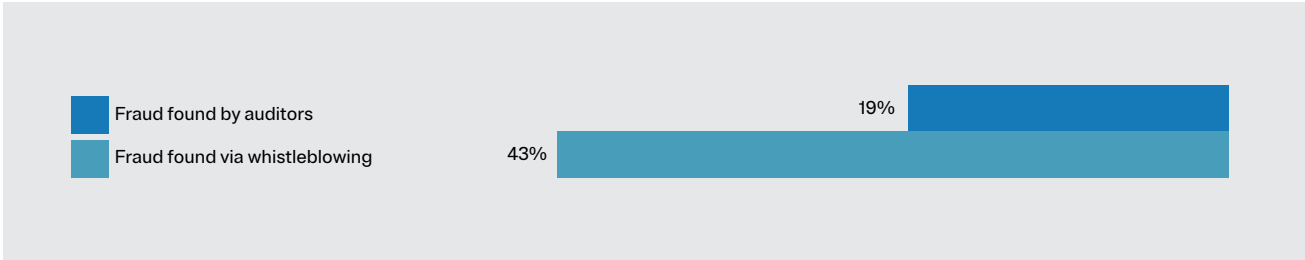
Adding to the complexity is the fact that this legislation takes the form of a Directive, and not a regulation. Regulations – like GDPR – apply consistently and immediately across all Member States. Directives, on the other hand, lay out a series of requirements and leave it up to each Member State to transpose into local law and thus decide how they will meet Directive requirements.

Introduction

While the Directive includes a deadline of December 17, 2021 for Member States to do so, it is not unusual for Member States to miss such deadlines. Though the Directive must be transposed into local law to become effective, it may still have limited direct effect (known as the vertical effect under EU law). This applies when provisions are what's termed "unconditional" – where the Directive's requirements are clear and precise and have not been transposed into national law by the required date.

When these conditions are met, individuals may rely on the Directive against an EU Member State in court. Though provisos and interpretation in court will determine the outcome of cases under these conditions, it is important to consider that Directive requirements are still effective – at least in part – without a local law in place.

All that said, companies should implement the unequivocal requirements of the Directive as soon as possible. Strategies for compliance with the Directive and local law can and should evolve as appropriate, recognizing the individual Member State implementations when they are published. This will certainly save last-minute work, and it will help companies take advantage of the natural benefits of having a hotline in place.



For example, 19 percent of fraud is found by auditors, but 43 percent is found via whistleblowing.

PLEASE NOTE:

This eBook does not constitute legal advice on the part of OneTrust. Over the past two years since the Directive was adopted, our team has invested considerable resources into understanding its requirements. We have researched, partnered with European compliance experts, and worked closely with customers to compile this guide. While our team does not provide legal advice, we can help companies implement a hotline that complies with Directive requirements on short notice. Please reach out to a member of our team for assistance with implementing a hotline.

What the Directive requires

In short, the Directive requires that companies provide internal mechanisms for whistleblowing, educate employees and others about their whistleblowing options, protect whistleblowers who report breaches of EU law, and prevent them from being retaliated against. It also includes requirements that Member States must follow - including establishing external reporting channels.

ESTABLISHING INTERNAL AND EXTERNAL REPORTING CHANNELS

More specifically, Article 8 of the Directive says that Member States must require legal entities in both the public and private sectors to establish reporting channels and mechanisms for follow-up. These mechanisms can be operated by a company employee or department, or by a third-party provider. Regardless, the reporting and follow-up procedures must meet the following Directive requirements:

- Protects the confidentiality of the reporter and the privacy of any third party mentioned in the report, and prevents access to the report by unauthorized team members
- Acknowledges receipt of the report within seven days
- Allows for diligent and impartial follow-up, communication, and feedback – including for anonymously submitted reports – within three months of the report's submission
- Allows whistleblower to review, approve, and edit initial report and subsequent interview notes
- Allows for reporting in writing, orally (through telephone or voice messaging, or a physical meeting if requested by reporter), or both
- Provides clear information on external reporting options

In addition to public and private entities, Member States also face new requirements under the Directive. They must establish external reporting channels. These external bodies face many of the same requirements as the internal reporting channels, plus they must:

- Communicate the final outcome of investigations to the reporter in accordance with Member State law
- Communicate the report and related information to the appropriate institutions and agencies associated with the European Union for further investigation, if needed

PREVENTING RETALIATION

The central aim of the Directive is to protect whistleblowers, namely from retaliation. For a deeper look at the anti-retaliation measures outlined in the Directive, see Chapter 6.

SUPPORT MEASURES FOR WHISTLEBLOWERS

The Directive requires Member States to provide whistleblowers and potential whistleblowers access to support measures. Information on whistleblowing procedures, protection from retaliation, and whistleblower rights must be available to the public for free. In addition, Member States must provide protected parties with access to legal aid in criminal and cross-border civil proceedings and may also provide financial aid and psychological support.

What the Directive requires

PENALTIES

Within the Directive, Member States are required to provide "effective, proportionate and dissuasive penalties" to anyone who attempts to hinder a report, engage in retaliation, bring vexatious legal proceedings against protected parties, or breaches confidentiality. In addition, those who knowingly report false information will also face penalties, and those affected by false reports may be entitled to damages.

CENTRAL REPORTING CHANNELS VERSUS INDEPENDENT CHANNELS FOR EACH SUBSIDIARY

While the Directive specifies that companies with between 50 and 249 workers may share resources for the purposes of reporting, there is – according to the EU Expert Group and the European Commission's interpretation of the Directive – no similar exception for group companies exceeding 249 workers. According to this interpretation, subsidiaries with 250 or more workers may no longer rely solely on their parent company's central whistleblowing systems, and must have the ability to investigate reports locally rather than at the group, or corporate, level.

"Subsidiaries with 250 or more workers may no longer rely solely on their parent company's central whistleblowing systems, and must have the ability to investigate reports locally rather than at the group, or corporate, level."

Central reporting channels and case management may still exist, but whistleblowers must have the option to report at the local or group level. Many large companies view this as impractical, and there are multiple potential risks associated with local reporting and investigation. In Denmark, leading multinationals have been working together to seek a change in how the legislation is implemented to allow for a more practical, centralized regime. Thanks to the corporations' successful lobbying, the Danish domestic law implementing the Directive has now been revised to allow companies to continue with their centralized systems, although there may be a challenge at some point. It remains to be seen how other Member States will transpose this requirement of the Directive.

What the Directive requires

FREQUENTLY ASKED QUESTIONS ON THIS TOPIC

1. What details regarding the outcome of the investigation must be provided to the reporter?

Recital 57 of the Directive states that feedback is a vital element of building up trust and reducing the need for further unnecessary internal or external disclosures. The recital requires that the employer's response should "as far as legally possible and in the most comprehensive way possible" inform the whistleblower of what happened or will happen because of their report. This could include referring the reporter to the grievance procedure (if that would be more appropriate), whether there was/will be an internal investigation, any remedial actions, any reports made to public authorities and/ or the status of the investigation, such as there being insufficient evidence to support the report. Each case and investigation will require assessment, and decisions to be taken regarding what can be disclosed, and what cannot; for example, there may be an ongoing and wider investigation which would limit what could be said in the timescales of the Directive.

Where the Directive applies, and to whom

The Directive will introduce an obligation on all companies, both public and private, with 50 or more employees, or with an annual turnover or total assets of more than €10M. Local authorities that provide services for more than 10,000 people are also subject to the Directive's requirements. Companies within these parameters are required by the Directive to set up internal processes for reporting and whistleblowing.

The Directive also applies to some companies that fall outside of these boundaries. Companies of any size that operate in Financial Services, or where there is a risk of money laundering or terrorist financing, must also heed the Directive's requirements to set up whistleblowing processes.

Also, this is a Directive, so there will be variations in whistleblower law across the 27 EU Member States. The Directive outlines minimum requirements, and Member States may choose to establish more stringent whistleblower protections.

"A lack of internal whistleblowing channels creates a real risk of employees (and others) reporting directly to regulators or the media, regardless of company size."

EU-BASED COMPANIES WITH EMPLOYEES OUTSIDE THE EU

While the Directive does not specify whether workers need to be physically located within the EU, it is reasonable to assume that any legal entity established in the EU that employs more than 50 workers will need to comply with the Directive, regardless of where the workers are located, be that inside or outside the EU.

COMPANIES BASED OUTSIDE THE EU WITH EMPLOYEES IN THE EU

Similarly, it is unclear whether non-EU entities that employ more than 50 workers within the EU will need to comply with the Directive. Given that their employees located in the EU are subject to a raft of EU labor laws, it is highly likely that such entities will be subject to the Directive, regardless of their employer's location.

Where the Directive applies, and to whom

FREQUENTLY ASKED QUESTIONS ON THIS TOPIC

1. Do we foresee these regulations having extraterritorial implications such as those for the GDPR?

It is quite possible to foresee a range of potential scenarios occurring where, for example, one company may have obligations to another regarding disclosures made under the Directive by an employee of another company. The European Commission's view is that the Directive has enough flexibility to be compliant with whistleblowing legislation in other jurisdictions, such as under the FCPA, although that is not fully clear at present.

2. There are always fluctuations in employee numbers throughout a period. If a company operates close to 50 (or 250) employees and shifts between, above, and below these thresholds, how is that managed?

In broad terms, the only difference in the Directive for companies with 50 and 250 employees is that of timing – although it is theoretically possible that in their implementations, some Member States might adopt a single date of December 2021.

If a company is around the 50-employee level, then it would be better to implement a whistleblowing capability because, for example, a lack of internal whistleblowing channels creates a real risk of employees (and others) reporting directly to regulators or the media, regardless of company size. It is also important to note that at least one Member State will reduce the threshold to 25 in their implementation.

3. Does the EU Whistleblower Directive apply in the UK?

It is worth noting that while most EU Member States have offered varying and fragmented standards of protection for whistleblowers, the EU did recognize that the UK already had comprehensive legislation in place to protect whistleblowers, namely the Public Interest Disclosure Act 1998 ("PIDA"). The UK Government has confirmed that it does not intend to adopt the Directive into UK law, given its departure from the EU, but many companies are including the UK in their implementation of the Directive.

4. As a global company operating not only in EU Member States, but also in non-EU Member states, are we obliged to comply with the EU Whistleblower Directive and implement helplines?

Assuming that your company has EU subsidiaries/ companies that meet the relevant employee thresholds (generally 50 or 250 employees) then yes, you will be obliged to comply with the Directive's requirements, including but not limited to providing internal whistleblowing helplines.

5. Does the employee count only include EU workers or US workers also?

EU only. However, it is important to note that the Directive does not specify whether workers need to be physically located within the EU, but it is reasonable to assume that any legal entity established in the EU that employs more than 50 workers will need to comply with the Directive regardless of where the workers are located, be that inside or outside the EU.

Who is protected by the Directive

The concept of a 'worker' in the EU is broad, and the protective scope of the Directive has been cast particularly wide.

It offers protection to all whistleblowers who have acquired information on violations of EU law in what is termed "a work-based relationship," regardless of the nature of their activities, whether it is paid, and whether or not they are EU citizens.

"It offers protection to all whistleblowers who have acquired information on violations of EU law in what is termed "a work-based relationship," regardless of the nature of their activities, whether it is paid, and whether or not they are EU citizens."

CONSEQUENTLY, THE DIRECTIVE PROTECTS:

1. Current and former (part- or full-time) employees
2. Directors
3. Non-executive directors
4. Temporary workers
5. Fixed-term contract workers
6. Sub-contractors
7. The self-employed
8. Freelancers
9. Suppliers
10. Vendors
11. Shareholders
12. Members of professional-type bodies
13. Job applicants
14. Work applicants
15. Trainees
16. Interns (paid or unpaid)
17. Volunteers
18. Third-parties or facilitators, such as colleagues or relatives, who could be affected by a disclosure report
19. Those whose workbased relationship has yet to begin, such as through pre-contractual negotiations, or leavers where it has ended

Who is protected by the Directive

Clearly, it's essential to create and communicate effective reporting channels and processes to support all the above, but the fact that third parties and relatives can be a whistleblower under the Directive means, for example, that external communications will be necessary, and a few posters put up in company bathrooms simply won't suffice.

External access to the hotline is also clearly going to involve considering aspects such as access outside the firewall, using your supplier or vendor portal and perhaps, specific phone numbers or email addresses.

FREQUENTLY ASKED QUESTIONS ON THIS TOPIC

1. Can a customer be a whistleblower?

In practice, yes.

However, the Directive does not specify them in its list of protected whistleblowers.

What types of whistleblowing are protected

The main goal of the EU Whistleblower Protection Directive is to help whistleblowers who aim to report breaches of EU law. Thus, protected whistleblowing under the Directive aligns with certain categories of law (though Member States may choose to add to this list).

THE FOLLOWING AREAS AND TOPICS ARE COVERED BY THE DIRECTIVE:

1. Public procurement
2. Financial services, products and markets
3. Product safety and compliance
4. Transport safety
5. Protection of the environment
6. Radiation protection and nuclear safety
7. Food safety; animal health and welfare
8. Public health
9. Consumer protection
10. Protection of privacy and personal data

> "In some cases, Member States are considering an extension to simply include 'suspicious wrongdoing,' which will be a significant increase in scope."

The EU is actively encouraging national lawmakers to extend coverage of wrongdoing to cover current national laws. In some cases, Member States are considering an extension to simply include "suspicious wrongdoing," which will be a significant increase in scope.

What types of whistleblowing are protected

FREQUENTLY ASKED QUESTIONS ON THIS TOPIC

1. Is there guidance available to assist companies in the case of a vexatious whistleblower, and what is the test of a proving such a whistleblower?

Companies will generally continue to use the disciplinary processes and standards of proof that they use today, which will include issues such as malicious whistleblowing reports, vexatious grievances, and more.

The Directive does, for example, reference that 'an important protection against malicious, junk or unreasonable reporting' is that 'persons who intentionally and knowingly reported incorrect or misleading information … do not enjoy protection.'

2. In EU countries that currently restrict issues that be reported, will the Directive open up/ standardize more issues as potential reporting categories?

Yes and no. Some Member States will potentially implement the Directive on a minimalistic basis, so that their national implementation only allows the specified breaches of EU law to be reported under the Directive. Other Member States will extend their implementation to cover breaches of national law, and others – such as the Netherlands and Sweden – will go further than that. So, while there will be some opening up of reportable breaches, how far that goes will vary given that there will not be EU-wide standardization.

How can whistleblowers submit reports

One of the fundamental shifts in the approach to whistleblowing that the Directive represents is its three-tier reporting structure.

THE THREE-TIER REPORTING STRUCTURE

1. INTERNAL CHANNELS

- Must be kept confidential
- Must be acknowledged within seven days and responded to within three months

2. EXTERNAL CHANNELS

- Competent authorities established by each member State
- Cases must be dealt with within three months (or within six months in justified cases)

3. PUBLIC

- Such as the media
- Reports may involve an imminent danger to the public interest, a risk of retaliation, or a failure to deal with concerns internally

> "You must, in order to empower potential whistleblowers, make your hotline as accessible as possible to all potential whistleblowers that are protected by the Directive."

Unlike previous laws in some Member States which required whistleblowers to report internally before going to regulators or the media, the Directive specifics that there is no hierarchy or order of operations with these three reporting methods. Whistleblowers will be protected by the Directive regardless of the route they choose. It remains in each company's best interest to encourage employees to raise concerns first via internal channels, stressing the confidentiality of those reports and the support that your organization can offer. The second tier enables employees to report concerns to external "competent authorities" at the EU or Member State level. The third tier enables whistleblowers to voice their concerns through the media or other high visibility means.

How can whistleblowers submit reports

REPORTING CHANNEL REQUIREMENTS UNDER THE DIRECTIVE

Meeting the spirit of the Directive is paramount here. You must, in order to empower potential whistleblowers, make your hotline as accessible as possible to all potential whistleblowers that are protected by the Directive. While the Directive specifies that reporting channels can be either written (through an online reporting platform, email, letter or complaint boxes) or oral (via telephone hotline, voice messaging system or in person), some Member States will require companies to provide both a written reporting option and an oral reporting option (Sweden was the first to enact this requirement). In order to not deter reporting, companies are expected to provide transparent information and clear, easily accessible reporting channels.

Accessibility is a key requirement of the Directive, and may look like providing intake in local languages, making your hotline available on a publicfacing landing page, and more. The more accessible your whistleblowing channels are, the more likely your employees, third parties, and others will be to rely on them rather than reaching out to external channels or the media.

FREQUENTLY ASKED QUESTIONS ON THIS TOPIC

1. Is it permissible to have two different online reporting mechanisms within the same company for different employees/job roles?

Is this compliant with the regulation, or is it advisable to have the same channel for all?

There is nothing in the Directive to exclude this, and some companies establish different reporting mechanisms for employees and suppliers/ vendors/ third parties. It's unclear whether separate channels for different employees and job roles would be beneficial; if reports require different handling, that can be readily achieved at the triage stage. A single channel may provide more consistent handling and comprehensive report data and analytics. If reports from different employees and job roles come via different mechanisms, then there could be greater potential for differences in case handling and, perhaps, disciplinary outcomes.

2. What is the recommendation if someone reports to a manager who is not the designated person?

Should the manager pass on to designated person or direct the reporter to do so?

Circumstances will vary on this issue. Sometimes a reporter will only be prepared to make their report to the manager who, for example, they may know or have worked with. In this situation – with the reporter's consent – the manager could pass on details of the report (often termed a 'proxy report') to the designated person.

Clearly, there are a range of circumstances – professional, personal, and other – where the manager might instead ask the reporter to contact the designated person, but it is always essential to weigh whether doing so might result in the reporter not making their report at all.

How can whistleblowers submit reports

3. Is one whistleblowing channel sufficient, or does the Directive require you to provide multiple channels?

The Directive states that 'the reporting channels should enable persons to report in writing and submit reports by post, by physical complaint box(es), or through an online platform, whether it be on an intranet or internet platform, or to report orally, by telephone hotline or other voice messaging system, or both. Upon request by the reporting person, such channels should also enable reporting by means of physical meetings, within a reasonable timeframe.'

However, the Directive also states that 'provided the confidentiality of the identity of the reporting person is ensured, it is up to each individual legal entity to define the kind of reporting channels to establish.'

So, to answer your question, there is no specific requirement to have multiple channels, but that decision is up to your company or your local Member State law – recognizing that some people may not necessarily be able to, or be comfortable with, making an online report for example.

It would be relatively easy to provide postal address(es) and complaint boxes to increase your channels, but complaint boxes, for example, can present several issues.

Some countries have different bodies and regulations (for example workers' councils, or grievance procedures in UK) that could conflict with a global hotline.

Does the Directive describe how concerns coming into the hotline should be managed in these cases?

The Directive does not refer to Works Councils. It does state that 'Member States could decide to provide that reports concerning interpersonal grievances exclusively affecting the reporting person, namely grievances about interpersonal conflicts between the reporting person and another worker, can be channeled to other procedures.' This is an example of the decisions devolved to Member States as part of their local implementation.

However, it should be stressed that this is a Whistleblower Protection Directive, such that employees may decide to make a hotline report rather than raise a grievance, because the Directive will potentially give themgreater protection from retaliation, mandated response timescales and other benefits.

Retaliation and the reverse burden of proof

Protecting whistleblowers from retaliation is at the heart of the EU Whistleblower Protection Directive. The impact of retaliation on an individual – and on the culture of a workplace – can be incredibly damaging. And many times, the retaliation is so subtle and insidious that other managers and employees are oblivious to it. The anti-retaliation requirements of the EU Whistleblower Protection Directive are a positive – and necessary – step forward for companies in the European Union.

Your company likely has an anti-retaliation policy in place, but it may not be enough to meet the new anti-retaliation requirements within the EU Whistleblower Protection Directive.

ANTI-RETALIATION REQUIREMENTS OF THE EU WHISTLEBLOWER PROTECTION DIRECTIVE

The Directive specifies that employees, former employees, subcontractors, shareholders, suppliers, and other third parties will be protected from dismissal, suspension, demotion, and other forms of retaliation in response to submitting a whistleblower report.

Additionally, those who support a whistleblower are also protected from experiencing retaliation.

The most significant anti-retaliation requirement within the Directive is the "reverse burden of proof." For the first time in a wide-ranging Directive, individuals are no longer required to prove that they have experienced retaliation. Instead, the company must prove that no retaliation has occurred. If they can't, they'll face penalties.

RETALIATION AS DEFINED BY THE EU WHISTLEBLOWER PROTECTION DIRECTIVE

Retaliation can take the form of "hard" or overt actions, or "soft" and subtle actions. The Directive defines retaliation broadly.

THE LIST OF RETALIATORY ACTIONS COVERED BY THE DIRECTIVE INCLUDES:

- 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

Retaliation and the reverse burden of proof

- Blacklisting based on 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

ANTI-RETALIATION "PROTECTIVE MEASURES" REQUIRED BY THE DIRECTIVE

The EU Whistleblower Protection Directive mandates that companies implement safeguards to prevent the above actions – plus more indirect forms of retaliation – and communicate those safeguards to their workforces and third parties. Additionally, the Directive requires that whistleblowers' identities be disclosed only to authorized staff members who are competent to receive and respond to reports. The same protection extends to those who assist and support whistleblowers and those who are implicated in whistleblower reports.

It is likely that under the Directive, whistleblowing cases will put scrutiny on what protective measures and anti-retaliation policies were in place at the time of the report, and how effectively they were deployed.

THE EU WHISTLEBLOWER PROTECTION DIRECTIVE'S "REVERSE BURDEN OF PROOF"

Under the EU Whistleblower Protection Directive's"reverse burden of proof" stipulation, companies must prove that whistleblowers have faced no retaliation as a result of their report. This is a unique and novel approach to retaliation.

Given the Directive's purpose of protecting whistleblowers, retaliation is a significant area of focus. The Directive presumes that when a whistleblower suffers some sort of detriment at work, that detriment exists as a form of retaliation to their report. Whereas previously whistleblowers have had to prove that they experienced retaliation, now employers and companies are accountable for proving that no retaliation has occurred.

HOW TO COMPLY WITH THE EU DIRECTIVE'S ANTIRETALIATION REQUIREMENTS

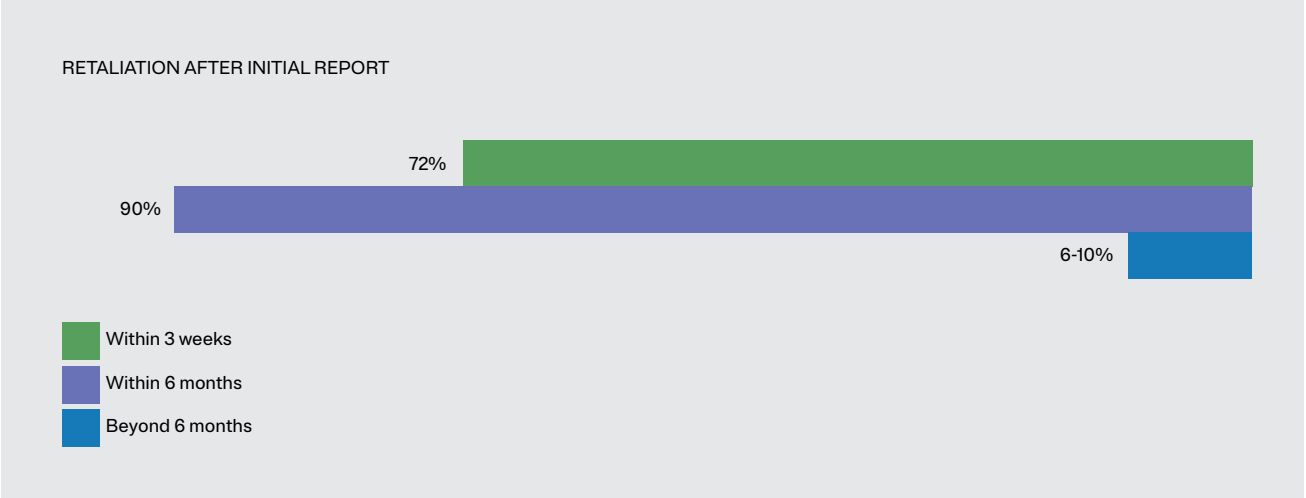
The Directive's reverse burden of proof calls for a proactive approach to preventing retaliation. The first step in complying with the EU Whistleblower Protection Directive's anti-retaliation requirements is to examine your current anti-retaliation policy. When you've ensured that your policy is comprehensive and up to date, communicate it to your workforce and all third parties using awareness campaigns. Where training is necessary – for high-risk individuals and managers, for example – ensure that those people are aware of your anti-retaliation policy and procedure, the requirements of the Directive, and the consequences for falling short.

Next, scrutinize the anti-retaliation processes that are already in place within your company to address retaliation as a result of whistleblowing.

Retaliation and the reverse burden of proof

For example, do you have analytics that can predict the risk of retaliation based on the report? Do you communicate anti-retaliation measures to those parties that may retaliate? Do you follow up with reporters? What is the timeline and process for following up, and what does your follow-up screen for? A retaliation risk assessment may be a helpful tool in benchmarking the current status of retaliation within your company. That process begins with establishing your markers of retaliation – for example, pay raises, performance reviews, and relocations – and establishing a "normal range" for each marker. Some markers can be measured with HR data, and some may require a highertouch approach; regardless, measure each marker against the reports you've received over the last year and make note of any outliers.

The data shows that 72 percent of retaliation occurs within three weeks of the initial report, and 90 percent within six months. However, with 6-10 percent of retaliation occurring beyond the six-month period, "once and done" follow-up won't detect some retaliation – let alone prevent it from happening. For more detail on effective anti-retaliation strategies, read our blog How to Support and Protect Whistleblowers.



"Companies must prove that whistleblowers have faced no retaliation as a result of their report. This is a unique and novel approach to retaliation."

Anonymity and confidentiality

Under the EU Whistleblower Protection Directive, the decision on anonymous reporting lies with each of the 27 EU Member States. Consequently, approaches to whistleblower anonymity will continue to differ, as they do now, based on local culture and history.

However, the Directive is quite clear on confidentiality. We'll dive into the subtleties of anonymity and confidentiality below.

ANONYMITY REQUIREMENTS OF THE EU WHISTLEBLOWER PROTECTION DIRECTIVE

While the Directive leaves anonymity requirements up to the Member States to decide, there are four primary approaches available to Member States:

1. No anonymous reporting

2. Only anonymous reporting

3. Anonymous reporting is allowed, but that ability is not publicized

4. Anonymous reporting is allowed, but companies are not obligated to investigate anonymous reports

> "Ensuring confidentiality requires scrutiny of the entire whistleblowing process from the point of a potential reporter accessing the relevant contact details of the hotline through to the report submission and on through case management, investigation, conclusion, and follow-up."

Currently, OneTrust offers a fifth potential option: a partially anonymous capability where reporters provide their details only to OneTrust while remaining anonymous to their employer. This ability is not yet accounted for in whistleblowing legislation anywhere in the world, but is an option available to our customers.

Anonymity and confidentiality

CONFIDENTIALITY REQUIREMENTS OF THE EU WHISTLEBLOWER PROTECTION DIRECTIVE

The Directive focuses extensively on confidentiality of whistleblowing reports and whistleblower identity – unsurprisingly, considering the aim of the Directive is to protect whistleblowers. Ensuring confidentiality requires scrutiny of the entire whistleblowing process from the point of a potential reporter accessing the relevant contact details of the hotline through to the report submission and on through case management, investigation, conclusion, and follow-up. Confidentiality has been broken in several high-profile cases (see the story of Wendy Addison for an example), and these occasions clearly influenced the thinking behind the Directive.

Confidentiality will require a selected and trained team of report handlers, supported by confidentiality and privacy policies, statements, and training.

Clearly, some reports must be shared outside this team, but policies, statements, and training all have a role to play in maximizing confidentiality for the reporter and the subjects of the report alike.

It can be difficult to maintain confidentiality in small companies or within small groups of employees, even with anonymous reporting. This issue should be recognized and proactively addressed to minimize the risk and consequences of a leak.

Communications, awareness, and training

If you have a whistleblower hotline – or a compliance program in general – employee awareness and training are likely not new concepts to you. However, the EU Whistleblower Protection Directive extends the scope of required awareness and training to all protected whistleblowers, and that includes contractors, vendors, and other third parties. It's worth reexamining your hotline awareness strategy and coming up with something that is effective, practical, and in line with Directive requirements.

TRAINING EMPLOYEES ON THE EU WHISTLEBLOWER PROTECTION DIRECTIVE

The Directive includes a requirement that employees and third parties are made aware of the Directive and the protections that whistleblowers are entitled to under it.

That training must cover the three-tier reporting provision – where reporters are protected whether they report internally to the company, externally to a regulator or other recognized institution, or externally to the media. This training can be folded into regular compliance training or stand on its own; either way, it must happen.

TRAINING CASE HANDLERS

More detailed training on the Directive may be limited to managers, case handlers, and groups who interact more closely with ethics and compliance initiatives. This training may cover the extended requirements of the Directive, variations across Member States, and anti-retaliation strategies.

EU DIRECTIVE REQUIREMENTS FOR HOTLINE AWARENESS EXTEND BEYOND EMPLOYEES

We've written several resources on raising hotline awareness and generating engagement with your compliance program – and those principles apply here as well. However, the Directive asks companies to consider a wider population than their employee base when it comes to hotline awareness. Therefore, it's worth looking at typical hotline awareness strategies through a new lens, one that includes vendors, contractors, interns, and more. Standard hotline awareness strategies include workplace posters, emails, and team briefings. Emails and meetings are easily expandable to your third-party work-based relationships. While workplace posters may be less visible to third parties, consider other materials that are passed back and forth through the course of business.

Can you include a pamphlet on the hotline alongside your invoicing materials? Consider your ethics and compliance program's online presence as well. If your Ethics and Compliance Portal is accessible outside the firewall, add a QR code for it to all your third-party communications, as well as to employee materials like pass cards, pay slips, and more.

EDUCATING YOUR BOARD OF DIRECTORS AND SENIOR LEADERSHIP

While the Directive doesn't require you to train your Board of Directors on whistleblowing,consider that the corporate liability which may result from the Directive may be essential information for them to have. Denmark's local whistleblowing law, enacted as a result of the Directive, includes a stipulation that companies will be fined for violations and could face criminal liability. The law also entitles whistleblowers to compensation.

These stipulations are a compelling justification when it comes to determining compliance budgets and other resourcing decisions.

Communications, awareness, and training

OVERCOMING REPORTING RELUCTANCE

When strategizing your hotline awareness communications, it's imperative to see things from the perspective of a potential whistleblower.

Address the key questions that will arise, like "Who will know about my report?" and "What will happen after I submit a report?" Proactively provide answers that can help address reluctance, and your awareness campaigns will be more effective.

ONE OF THE MAJOR BARRIERS TO REPORTING IS FEAR OF THE UNKNOWN. CONSIDER A FEW MEASURES TO ADDRESS IT:

- Try branding your hotline or giving it an identity. OneTrust customers have had success with brands like "Talk to Peggy" or "Ask Veronica." This humanizes the hotline and reduces the perception that reports are submitted to a nameless agency.
- Use reassuring imagery (one OneTrust customer used posters of dogs) in awareness campaigns to make the hotline recognizable while subliminally reassuring viewers.

"When strategizing your hotline awareness communications, it's imperative to see things from the perspective of a potential whistleblower."

- Run a simple competition that invites employees and those with work-based relationships to submit a test report. Everyone who participates is entered in a raffle. Through submitting a test report, each potential whistleblower gains practice and becomes familiar with the reporting process.
- Define the terminology associated with whistleblowing, like "anonymous" and "confidential."

Communications, awareness, and training

FREQUENTLY ASKED QUESTIONS ON THIS TOPIC

Do companies need to provide employees and third parties with the specific regulator contact information?

Yes. Training and communications (for employees and others) are central to the Directive's requirements and, clearly, questions such as "were you given information" and "were you trained" are certainly going to be asked in the event of an investigation. While many of the regulatory bodies are still being established, the Directive is clear on this issue.

How do I know which external regulator to point a reporter to? Is there a resource for identifying the relevant external regulating entity in each country for each of the laws covered by the Directive?

Some Member States have a nominated ministry/regulator/agency (some may potentially have more than one), but others are still in the process of deciding their approach, usually linked to their publication of the implementation of the Directive. So yes, you will need to provide reasonable contact details. There is no source for this at present, but there undoubtedly will be.

Data Privacy and GDPR

Invariably, whistleblowing hotlines handle and process personal data. The EU Whistleblower Protection Directive requires that such processing take place in compliance with EU data protection law, namely the General Data Protection Regulation (GDPR). GDPR does not specifically reference whistleblowing – but that doesn't mean whistleblowing is any less protected. The potential risks to reporters and subjects of a report can't be overstated, so data protection is crucial for all parties involved.

PROCESSING WHISTLEBLOWER DATA

There are essentially two legal bases for processing personal data in the context of whistleblowing. These are generally:

1. The processing is necessary for compliance with a legal obligation, or

2. It is deemed to be a 'legitimate interest' of the controller, company or third-party.

Clearly, transposition of the Directive in the individual Member States will result in the first legal basis becoming effective. There has been, and will continue to be, reliance on 'legitimate interests' for a range of activities associated with whistleblowing.

> "When strategizing your hotline awareness communications, it's imperative to see things from the perspective of a potential whistleblower."

Clearly, the nature of some whistleblowing reports may involve what is termed 'special categories of personal data', which will require additional precautions, including confirmation that the processing is legal.

THE RIGHTS OF DATA SUBJECTS, BOTH WHISTLEBLOWERS AND REPORT SUBJECTS

Confidentiality is central to the operation of any whistleblowing program – confidentiality both for reporters and the subjects of their reports. A key element of discharging these rights includes publishing notices and policies which include transparent information on the hotline process, including how it operates, who will be involved, and how the rights of data subjects can be exercised. Clearly, there can be complexities in whistleblowing where, for example, responding to a Data Subject Access Request could jeopardize an investigation or expose a whistleblower. This type of scenario is generally reflected in GDPR's provisions and exceptions regarding the collection of personal data – and allows for responses to be delayed for as long as the risk exists. In a similar vein, the exercising of rights such as data erasure may be restricted to protect the rights and freedoms of others affected by the reporting.

Data Privacy and GDPR

DATA CONTROLS AND SECURITY UNDER GDPR AND THE EU DIRECTIVE

Data controllers are required to implement controls and provisions to ensure the security of personal data obtained during the whistleblowing process. This includes ensuring the reporter's identity is not disclosed either accidentally or illegally. Organizational provisions, for example, can ensure that only a limited number of designated people have access to report data – and that such data is only shared with those who need it to investigate and manage reports.

For multi-national companies where there may be a requirement to transfer report data within and beyond the EU, GDPR remains in effect and its data transfer restrictions must be recognized. Under the EU Whistleblower Protection Directive and GDPR, any data processors used in the whistleblowing process, including third parties, must have in place the necessary contractual provisions and be compliant with all relevant regulations.

LOOKING FORWARD

The EU Data Protection Board (EDPB) may issue new guidance on the relationship between GDPR and the EU Whistleblower Protection Directive. In the meantime, companies will have to rely on industry bodies, local regulators, external advisors, and their own knowledge of data protection as they implement the Directive's requirements.

FREQUENTLY ASKED QUESTIONS ON THIS TOPIC

Sweden's local whistleblowing law requires companies to delete the personal identifying information (PII) of the reporter after 60 days if there isn't any disciplinary action or litigation as a result of the investigation. Does this requirement also apply to the subject's PII?

That requirement isn't universal across the EU Member States but, crucially, there also wider considerations here. Briefly, some 72% of retaliation occurs within 3 weeks of a report being made, 90% within 6 months and 6% to 10% beyond 6 months. So, deleting the PII after 60 days could mean that the original report is deleted before the report of retaliation comes in.

Not surprisingly, the practicalities of retaliation aren't generally considered in relation to data retention legislation.

How are companies dealing with data privacy concerns if they have EU and non-EU subsidiaries that operate under different local or central regulations?

Companies currently transfer whistleblowing, legal, compliance and HR-related data to other Member States within the EU, and also to non- EU countries, and those processes, regulations and laws (such as GDPR) will continue to apply, as of now, under the Directive. Whilst there are continuing global developments regarding data protection, the Directive itself does not change these.

Finding a hotline vendor to help you comply

Does your current hotline provider – if you have one – stand up to the scrutiny necessary to comply with the EU Whistleblower Protection Directive?

Beyond the requirements of this Directive in particular, consider that whistleblower regulations and privacy regulations are evolving at a rate never seen before. Perhaps the most essential element to consider as you evaluate vendors is how well they are positioned to adapt, evolve, and stay ahead of the ever-changing whistleblowing landscape. Evaluate potential hotline vendors or your current provider against the key hotline requirements of the Directive.

HOTLINE REQUIREMENTS:

1. Subsidiary-level intake channels and case management

2. Reporter communication: anonymous and named

3. Data security and GDPR

4. Call center

5. Accessible intake methods

6. Confidentiality and retaliation prevention

7. Record keeping and retention

SUBSIDIARY-LEVEL INTAKE CHANNELS AND CASE MANAGEMENT

The EU Commission has been quite clear that subsidiaries with 250 or more workers may no longer rely solely on their parent company's central whistleblowing systems, and must have the ability to investigate reports locally rather than at the group, or corporate, level. Central reporting channels and case management may still exist, but whistleblowers must have the option to report at the local or group level.

Choose a hotline provider that can set up dedicated intake channels and case management for each subsidiary, in addition to the central/ corporate-level intake and case management. Clarify with your vendor whether you will be able to maintain visibility into trends and company-wide risk areas while keeping case-level data separate.

REPORTER COMMUNICATION: ANONYMOUS AND NAMED

The Directive requires a few things when it comes to communicating with whistleblowers. These are:

- Acknowledgment of receipt within seven days

- Ability to take anonymous reports

- Ability to communicate with reporters, anonymous or not

- Resolution/feedback within three months

- Diligent follow-up

- Ability for whistleblower to review, approve, or edit interview notes

Bear in mind that the Directive establishes the floor, carving out the minimum requirements for protecting whistleblowers. Your organization's actual plan can (and perhaps should) go above and beyond the letter of the Directive. Your compliance team should communicate with whistleblowers and document as much as possible in order to establish trust and transparency. A hotline provider should be able to automate some of the process using a workflow, making sure that your communication and documentation adheres to the Directive's requirements without introducing an insurmountable workload.

Finding a hotline vendor to help you comply

DATA SECURITY AND GDPR

Remember that 2016's General Data Protection Regulation (GDPR) came from the same governing body, and the guidance adopted by all Member States also needs to be honored in your efforts to comply with the EU Whistleblower Protection Directive. This means prioritizing the same issues (secure communications, minimal personal identifying information, authorized access to records, etc.) and keeping up with the same standards. Your organization will have to scope out exactly how much necessary information you need to collect, and how long you archive that sensitive data, in order to process your reports, while remaining compliant with GDPR. Require the following of your hotline vendor:

- GDPR compliance
- Collection of only the necessary personal information required to handle the specific report
- Secure and confidential reporting channels
- Prevention of access by non-authorized employees

CALL CENTER

The Directive requires that your whistleblowing intake channels are accessible to all protected parties. "Accessible" is up for interpretation, so choose a hotline vendor that uses a call center capable of processing reports in multiple languages, regardless of internet access or physical location. The Directive is clear that any person who acquires information from business activities can be a whistleblower, not just current full-time employees, so a well-trained and capable call center is key for expanded reporting. Require the following from your vendor's call center:

- Language capabilities
- GDPR compliance
- Competent, knowledgeable, and able to communicate the investigative protocol
- Available and accessible to employees, subsidiary employees, suppliers, agents, and any persons who acquire information through work-related activities
- Competent, independent, and empathetic
- Professionally trained to handle whistleblowing reports

ACCESSIBLE INTAKE METHODS

A call center is one channel for establishing accessible intake. Depending on the size of your organization and the scope of your international operations, you may seek to establish more than one intake method. According to the Directive, your reporting channels "should be made available to employees, subsidiary employees, suppliers, agents, and any persons who acquire information through work-related activities."

Establishing multiple routes for employees to speak up means that you're honoring the accessibility component of the Directive, and you are also reinforcing trust and transparency at your organization. Be thoughtful when considering your vendor's capabilities for report intake, because they matter on multiple levels, and flexibility will be key as Member States may choose to require different approaches to intake options.

Finding a hotline vendor to help you comply

OneTrust's flexible intake options include:

- Web
- Email
- Line manager (proxy)/physical meeting
- Whistleblowing hotline, available by telephone or voice messaging

ACCESSIBLE RESOURCES

Beyond establishing accessible intake methods, you must make sure that whistleblowers are provided with the necessary resources. Think your process through, from what initial intake looks like to how case resolution will be operationalized. Does the process include resources, education, and enablement for whistleblowers? In practice, all organizations should have a dedicated whistleblowing website or intranet page. Does the vendor you're considering offer such a feature? This resource page should contain, or link to:

- An introduction from senior stakeholders/ appointed representatives
- Contact and helpline information
- External resources and support
- Policies, procedures and training materials
- Positive testimonies
- Whistleblowing metrics
- Employee code of conduct
- Information on protection
- Frequently asked questions (FAQs)

CONFIDENTIALITY AND RETALIATION PREVENTION

There is a strong tie between confidentiality and retaliation prevention. Inherently, the more confidential a whistleblower report can be kept, the less likely the reporter is to be retaliated against. There is a dual obligation here; does your helpline ensure confidentiality, and does it help you prevent retaliation? With the new emphasis on the reverse burden of proof for retaliation, your efforts here will end up saving you time and effort down the road and you may be navigating away from costly sanctions or legal sanctions at the same time.

Require the following of your hotline vendor:

- Ensures confidentiality of persons reporting and third parties mentioned
- Allows full confidentiality unless otherwise required by national law
- Enables "diligent follow-up" with reporters, even if anonymous
- Retaliation prevention and monitoring through follow-up and screening

RECORD KEEPING AND RETENTION

Have you ever tried to access the email inbox of a former employee, only to be met with impossible logins and roadblocks? The Directive emphasizes retrievability because of issues like this. Every report must be dealt with by competent staff, ensuring that sensitive documents are only accessed by trained individuals and competent authorities.

Finding a hotline vendor to help you comply

The following points are best practices to ensure that your records are kept safe, compliant, and retrievable, so consider these when evaluating vendors:

- Every report is retrievable
- Reports can be forwarded to competent staff without modification
- Complete and accurate meeting notes kept in durable and retrievable form
- (recording or staff notes)
- Should offer the reporting person the opportunity to check, edit, and agree on the minutes of the meeting by signing them
- Reports can be used as evidence in enforcement actions
- If phone call is recorded, recording must be kept or transcribed
- If unrecorded, must be able to document the oral reporting in the form of accurate minutes of the conversation written by staff member

EU WHISTLEBLOWING PROTECTION DIRECTIVE HOTLINE VENDOR CHECKLIST

When you're evaluating vendors to help you with everything mentioned above, there are some important tactical items to consider. The devil is, indeed, in the details and translating to-do items into action can be an uphill climb. Use each of the lists above, along with the best-practices checklist below, as you evaluate vendors between now and the deadline to ensure that your hotline vendor serves your organization's unique plan and goals.

- Define roles & responsibilities and key milestones
- Geographical scope (territories, languages, entities)
- Define reporting categories. What is in, what is out?
- Decide anonymous reporting
- Decide on internal only or also opening to third parties and public
- Data privacy (GDPR): ask for certificate and pen test reports
- Translation options
- Attachments possible
- Two-way communication possible
- Decision on reporting channels (hotline only or email and external lawyer on top?)
- Ask for: territory credentials, industry credentials, local resources, benchmarking
- Ask for cost drivers and transparency
- Dashboard for board reporting
- Data upload possible from other sources
- Customized landing page

About OneTrust

OneTrust's flexible, multi-channel Helpline & Case Manager solutions empower companies across Europe to comply with the requirements of the EU Whistleblower Protection Directive and their local Member State law. Our human-centric intake enables easy reporting and efficient case management, while protecting whistleblowers from retaliation. Plus, we can help you make the switch to our Helpline and Case Manager quickly.

HELPLINE & CASE MANAGEMENT PRO

For companies looking for fast implementation and an easy-to-use, easy-to-configure helpline and case management solution

- Supports up to 2,000 employees
- Anonymous web and interactive voice response (IVR) intake
- Automated triage: Get the right reports to the right people
- Flexible, cost-effective contracts
- Self-configurable intake and case manager
- 20 languages supported for admins and reporters
- In-app reporting on case volume trends
- Built-in data privacy and information security

HELPLINE & CASE MANAGEMENT ADVANCED

For maturing companies looking for sophisticated tools and features to advance your speak-up program

- Multi-channel global intake
- Global call center and toll-free lines
- Robust language support and real-time translations
- Automated triage: Get the right reports to the right people
- Advanced case management
- Communicate with reporters
- Multiple anonymity options
- Retaliation prevention and monitoring
- In-app case-level reporting
- Built-in data privacy and information security

HELPLINE & CASE MANAGEMENT ENTERPRISE

For companies with large reporting volume who need deeper risk visibility, rich analytics, and board-ready reporting

- Multi-channel global intake
- Global call center and toll-free lines
- Robust language support and real-time translations
- Automated triage: Get the right reports to the right people
- Communicate with reporters
- Multiple anonymity options
- Retaliation prevention and monitoring
- Integrated data and analytics with boardready reporting
- Built-in data privacy and information security

onetrust

As society redefines risk and opportunity, OneTrust empowers tomorrow's leaders to succeed through trust and impact with the Trust Intelligence Platform. The market-defining Trust Intelligence Platform from OneTrust connects privacy, GRC, ethics, and ESG teams, data, and processes, so all companies can collaborate seamlessly and put trust at the center of their operations and culture by unlocking their value and potential to thrive by doing what's good for people and the planet.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

2020 Update to the Evaluation of Corporate Compliance Programs

"It's taking business intelligence and putting it into compliance."

- Jonathan Marks

UPDATED JULY 2022

Table *of Contents*

Part 1: Key Themes 3

Part 2: Data, Continuous Monitoring, and Continuous Updating..... 4

Part 3: M&A and Third Parties 6

Part 4: CCO & Compliance 7

Part 5: Renewed Importance of Compliance..... 8

OneTrust
PRIVACY, SECURITY & GOVERNANCE

In June of 2020, the Department of Justice (DOJ) released an update to its 2019 Evaluation of Corporate Compliance Programs. Moving forward, this new document will be called the 2020 Update. The 2020 Update is welcome news for every Chief Compliance Officer (CCO), compliance professional, and corporate compliance program in the US and beyond. The reason is simple: It ends, once and for all, the clarion call for paper compliance programs written by lawyers for lawyers. The DOJ has now articulated what both the business and compliance communities have been learning: Compliance is a business process, and as a process, it can be measured, managed, and most importantly, improved. Read on to explore the 2020 Update.

NOTE: All changes from the 2020 Update are noted in ***italics and bolded***.

Part 1: Key Themes

In the introduction, the DOJ now states, "Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a ***reasonable***, individualized determination in each case ***that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program."***

This change makes clear that every policy will be evaluated on its own merits. The DOJ lays out some of the factors it will consider, but such consideration will be tempered by a reasonableness standard. Borrowing language from the Antitrust Division, the 2020 Update adds that any compliance program under evaluation by the DOJ will be considered ***both at the time of the offense and at the time of the charging decision and resolution.*** The significance of this cannot be overstated, as now you cannot simply remediate your compliance program and basically ask for forgiveness after the Foreign Corrupt Practices Act (FCPA) violation has occurred. This statement clarifies any confusion generated by the Benczkowski Memo that all you have to do is aggressively remediate and such post-event cleanup will lead to a declination.

This point is further driven home by the addition to fundamental question Number 2, requiring prosecutors to ask, "Is the program being applied earnestly and in good faith?" In other words, is the program ***adequately resourced and empowered to function effectively?*** By tying this new language to question Number 2, companies that want to cut back to a paper program and take away the ability of a CCO to effectively do their job will lose the credit going forward, as this language clearly references both monetary resources and headcount.

The final addition in the introduction adds the following language: "In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue and the ***circumstances of the company."*** This addition emphasizes the importance of consistent and reliable documentation. For example, be prepared to explain why your company makes any changes to your program, loses headcount, or is not allowed to use the most current tech solution. The only way to do so is through a clearly-articulated business justification. You should plan to take this a step further and document how your solution follows compliance guidance as robust as the 2012 FCPA Guidance, issued by the DOJ and Securities and Exchange Commission (SEC). This section also allows room for creativity and imagination in your compliance program, if you can justify it and there is documentation for it.

From the changes in the tactical information presented in the

2020 Update, it is clear that the DOJ expects a continually-evolving compliance program. This clearly demonstrates how the days of a paper program are dead. This also separates the DOJ analysis away from the approach in ISO 37001, which is also a paper program approach to compliance. The 2020 Update suggests the use of a variety of compliance tools, in order to gather information and work those findings into your compliance program on an ongoing basis. This will ensure that your program is dynamic and constantly evolving, rather than remaining static and totally dependent on fixed policies and procedures.

Your risk assessment, so much more than the starting point for continuous improvement in your compliance program, now needs to shift from a once-every-three-years undertaking into a frequently referenced and revised position. Your risk assessment will reveal how to design, create, and implement your compliance program and will also serve as the documentation and justification for related decisions. The 2020 Update specified, ***"In short, prosecutors should endeavor to understand why the company has chosen to set up the compliance program the way that it has, and why and how the company's compliance program has evolved over time."***

Your compliance program, continuously improving and evolving, needs to be informed by more sources of information outside the scope of your risk assessment, such as your policies and procedures. Your policies and procedures need to be formatted for easy search and must be able to accurately track views. The 2020 Update stated, ***"Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?"***

As compliance evolves, the 2020 Update will be seen as a key demarcation where the government demonstrated that properly viewed compliance is more than a business process, it is a business program.

Part 2: Data, Continuous Monitoring and Continuous Updating

Shifting focus to the biggest modifications of the 2020 Update, tactical steps must be taken in order to move towards the twin concepts of continuous monitoring and continuous improvement. The changes began in Section 1: Risk Assessments, which stated:

Updates and Revisions

Is the risk assessment current and subject to periodic review? ***Is the periodic review limited to a "snapshot" in time, or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures, and controls? Do these updates account for risks discovered through misconduct or other problems with the compliance program?***

Lessons Learned

Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region?

The question-by-question analysis begins with ***"Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions?"*** Do you have access to continuous and real-time transactional data at your organization? How about across silos within your organization? Most likely the answer to both is "no." This answer means that, at this point in time, your compliance program is not informed by best practices.

If you find yourself in this situation, how do you begin to address it? Start with your highest risk activity, which will most likely be sales. Go to each point in the sales cycle: (1) Prospecting, (2) Contacting, (3) Qualifying for Tender Process, (4) RFQ and RFP, (5) Contract Negotiation, and (6) Contract Execution. Pull data related to compliance from each one of these data points and begin

your updated risk assessment there. The next question found in the Updates and Revisions subsection ties into the sole question found in the Lessons Learned subsection. They both relate to the single inquiry of how you used the data: Did you incorporate your findings into updating your compliance program?

While there is only one question in the Lessons Learned section, it is a compound question. It not only inquires about data you may have obtained through your own work, but also from other companies in your industry, operating in the same region. Without commenting on the potential anti-trust aspects of this issue, if there is public source information available to you (and there always is), how are you using this information in your compliance regime? This can look like asking your fully-operationalized employee base to keep their eyes and ears open at trade shows or any other gatherings of industry employees.

Also embedded in these two questions is another old theme in compliance: Is there sufficient documentation in your compliance program? Remember, the goal here is to document the basis for your decision, then explain your decision-making calculus. No compliance professional, compliance program, or even a company under Foreign Corrupt Practices Act (FCPA) investigation or scrutiny has ever been punished for making an incorrect decision where a sufficient and documented business justification was in place. Such entities and persons have been sanctioned when there was no documentation in place.

Policies and procedures, not traditionally associated with continuous monitoring and continuous improvement, are the next areas of focus. Here the 2020 Update stated:

Design

What is the company's process for designing and implementing new policies and procedures and ***updating existing policies and procedures,*** and has that process changed over time? Who has been involved in the design of policies and procedures? Have business units been consulted prior to rolling them out?

Accessibility

How has the company communicated its policies and procedures to all employees and relevant third parties? If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees' access? ***Have the policies and procedures been published in a searchable format for easy reference? Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?***

When was the last time you updated your policies and procedures? More importantly under the 2020 Update, what was your process for doing so? Was there any rigor around your process? Did that rigor include incorporating information and data collected through continuous monitoring, real-time monitoring, or continuous access to operational data and information across functions? For the first time, the 2020 Update asks if you have tracked who is looking at your policies and procedures and where they are located as data points for you to consider in updating your compliance program.

The final area in the 2020 Update for consideration is appropriately called Continuous Improvement, Periodic Testing and Review and is found in the subsection called Evolving Updates. It reads:

How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries? ***Does the company review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks?***

Similar to the language under Risk Assessment, this compound question considers the adaptation of a compliance program from your own lessons learned, but also from other companies. Take special note of the phrase, "other companies facing similar risks." Think about how this language would apply to any company operating in China, West Africa, or any other high-risk region in the globe. This could be interpreted to mean every CCO and compliance practitioner needs to stay abreast of international anti-corruption enforcement actions where your company may be doing business.

Part 3: M&A and Third Parties

Next, consider the changes in the areas of mergers & acquisition (M&A) and your third-party risk management protocols.

Mergers and Acquisitions

Under M&A, the 2020 Update stated: "A well-designed compliance program should include comprehensive due diligence of any acquisition targets, ***as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls. Pre-M&A due diligence, where possible,*** enables the acquiring company to evaluate more accurately each target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete ***pre- or post-acquisition*** due diligence ***and integration*** can allow misconduct to continue at the target company, causing resulting harm to a business's profitability and reputation and risking civil and criminal liability."

The specific questions posed by the 2020 Update are:

- **Due Diligence Process** – Was the ***company able to complete pre-acquisition due diligence and, if not, why not?*** Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities, and how was it done? What is the M&A due diligence process generally?
- **Integration in the M&A Process** – How has the compliance function been integrated into the merger, acquisition, and integration process?
- **Process Connecting Due Diligence to Implementation** – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures, and conducting ***post-acquisition audits***, at newly acquired entities?

The clear emphasis of the DOJ is around the pre-acquisition phase in M&A work. Were you prevented from engaging in pre-acquisition due diligence because of some rule or regulation? If so, what did you do about it? Did you take the approach of Halliburton, as it did in the resulting Opinion Release 08-02, and seek DOJ input? Was your post-acquisition integration protocol more robust? If so, how? Also, after closure, did you perform a full audit of the acquired entity?

Pre-acquisition due diligence provides an early assessment, informing the transaction research and evaluation phases. This could include an objective view of the risks faced and the level of risk exposure, such as best/worst case scenarios. A pre-acquisition risk assessment could also be used as a lens to view the feasibility of the business strategy and help to value the potential target.

The next step is to develop the risk assessment as a base document. From this document, you should be able to prepare a focused series of queries and requests to be obtained from the target company. Thereafter, company management can use this pre-acquisition risk assessment to attain what might be required in the way of integration, post-acquisition. It would also help to inform how the corporate and business functions may be affected. It should also assist in planning for timing and anticipation of the overall expenses involved in post-acquisition integration. These costs are considerable and they should be thoroughly evaluated in the decision-making calculus.

Third Parties

Even in 2020, third parties represented the highest risk under the Foreign Corrupt Practices Act (FCPA). Here the DOJ noted, "Prosecutors should also assess whether the company knows ***the business rationale for needing the third party in the transaction, and the risks posed by third-party partners, including*** the third-party partners' reputations and relationships, if any, with foreign officials… In sum, a company's third-party ***management*** practices are a factor that prosecutors should assess to determine whether a compliance program is, in fact, able to "detect the particular types of misconduct most likely to occur in a particular corporation's line of business."

The DOJ then posed the following questions:

- **Management of Relationships** – How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? How does the company monitor its third parties? Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past? How does the company train its third-party relationship managers about compliance risks and how to manage them? How does the company incentivize compliance and ethical behavior by third parties? ***Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?***

The new final question, coupled with the new language in the preamble to the section on third parties, is significant. It makes clear that management of third parties is a process, one that must continue on an ongoing basis, throughout the lifetime of the relationship with your organization. From the compliance perspective, this also re-emphasizes the importance of managing the relationship after the contract is executed. Your role in the compliance function is not simply to review due diligence and add compliance terms and conditions to the contact; your role is to oversee the relationship that the business sponsor manages on the ground, fully-operationalizing your compliance regime.

Part 4: CCO & Compliance

Next, consider the two clear winners in this 2020 Update: the emphasis on the CCO and the compliance function.

Quality of CCO and Compliance

Under Part II, the changes started with the title of the section which was amended to read "II. Is the Corporation's Compliance Program ***Adequately Resourced and Empowered to Function Effectively?***" This change was then driven home immediately in the introductory paragraph. "Even a well-designed compliance program may be unsuccessful in practice if implementation is lax, ***under-resourced***, or ***otherwise ineffective***." The introduction also added language from the US Sentencing Guidelines which reads, "(those with 'day-to-day operational ***responsibility' shall have 'adequate resources, appropriate authority and direct access to the governing authority or an appropriate subgroup of the governing authority'***)."

This builds upon the changes, started in the DOJ's 2016 FCPA Pilot Program and the 2017 FCPA Corporate Enforcement Policy, around the quality of your CCO and compliance function. It begins with questions such as: What is the overall corporate investment in compliance? Is your spend in line with similarly situated organizations? What about the salaries of your CCO and compliance personnel? Does your organization skimp on them to save money?

The new queries posed by the 2020 Update in this area are:

- **Experience and Qualifications** – Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities? Has the level of experience and qualifications in these roles changed over time? ***How does the company invest in further training and development of the compliance and other control personnel?*** Who reviews the performance of the compliance function and what is the review process?

Clearly, there must be ongoing professional development for the CCO, compliance team members, and other control personnel in the company. As a leader, every CCO should work with their compliance team to set up a clear path for career development and, more importantly, specific compliance subject matter expertise (SME), including the latest developments in compliance and evolving best practices. As a CCO, It also means you have to do the same development.

What about the phrase "other control personnel" and who is this group? Any compliance program embracing industry best practices should also advocate for the use of the non-compliance function as a gatekeeper. Any person at your company who makes decisions regarding compliance issues is included in this list: the legal department, compliance function, supply chain, human resources, payroll and/or internal audit.

To ascertain how decisions and actions are taken regarding

compliance issues, look beyond paper line reporting and assess lines of communications and information reporting structures. When it comes to budget and spend, for example, it is important to understand who authorizes compliance expenditures; the CCO, the Board or Audit Committee, or the Chief Executive Officer (CEO) or perhaps other(s).

Moving the company to a point where DOJ requirements are met may be a difficult process; If gatekeepers believe that they understand compliance, but have very little appreciation for best practices, doing compliance, or the operationalization of compliance, their uninformed views will require you to tread lightly. You will need to determine if these gatekeepers will defer to the CCO and compliance SME or outside consultants as SMEs. The optimal situation is where the gatekeepers are highly knowledgeable but are willing to defer to the CCO as the compliance SME.

Data, Data, Data

The second area of inquiry is the access to and use of data, data analytics, and transaction monitoring by the compliance function.

- **Data Resources and Access –** ***Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?***

This set of queries is not simply phrased in the negative but it requires a company to work to make such data available to the CCO and compliance function. This is a much more stringent requirement than the CCO calling up IT to find out what data might be available to monitor on an ongoing basis. These questions require every company to take affirmative steps to make the data available and format the compliance data into some type of usable format.

Finally, this inquiry ties back to the part of the title of Part II referenced above, which requires that a CCO and compliance function "be empowered to function effectively." Moving forward, the requirement for accessibility to siloed data and its use by compliance will be critical in the business world. Compliance is truly at an inflection point: The 2020 Update will drive compliance functions towards more and greater use of data in compliance going forward.

Part 5: Renewed Importance of Compliance

Coincidence or not, the timing of the 2020 Update makes clear the importance of compliance as a regulatory scheme to comply with laws such as the FCPA. Some have called for a hiatus on compliance, so companies can get back on their feet after the worst economic downturn since the Great Depression and the worst pandemic in over a century. Those commentators advocate that it is somehow acceptable to override compliance and financial controls because our unprecedented times. Such thinking was wrong then and it's wrong now. Bribery and corruption under the FCPA have been illegal since 1977 and remain so today. Compliance programs are the way to operate within the boundaries of the law and this is even more true now.

The push around data, ongoing monitoring, and continuous improvement of compliance programs also re-emphasizes that compliance is now properly seen as a business process and is no longer the purview of lawyers and the legal department. Compliance is there to ***prevent, detect, and remediate*** issues before they become full-blown legal violations. This call for increased improvement of your compliance program, on an ongoing basis, will eventually lead to more thorough and robust transaction monitoring by organizations. By doing so, companies will have the opportunity to make their business processes and operations more efficient and, at the end of the day, more profitable.

While many commentators have focused on the section of 2020 Update that mandates that the compliance function have access to data throughout the organization, the point is that there is a plethora of unused data available to a CCO and company. Obviously, hotline complaints are a rich source of data and can

be used in a variety of ways. But the 2020 Update also spoke to questions raised about policies and procedures. Where did those questions come from? Who in the company raised them? Who in the company is accessing your policies and procedures, and in what geographic region are they located? What does that tell you about your compliance program? If you cannot travel for some period of time due to COVID-19, you should identify ways to assess and address the questions the customers of your compliance program (i.e., employees) are raising.

The same types of analysis can be true for other information. Where are your Corporate Social Responsibility (CSR) initiatives located? Are they in high-risk jurisdictions? What visibility do you have into them before the money is spent? What about marketing budget spends? Any large expenditures in high-risk jurisdictions? What about hiring? When was the last time you looked at your organization's hiring in high-risk jurisdictions? All of these could provide information that can be incorporated back into your compliance program.

The final aspect from the 2020 Update was first raised by Dick Cassin. The question Cassin cited was "Does the compliance function monitor its investigations and resulting discipline to ensure consistency?" Cassin went on to add, "Why is the added emphasis on monitoring to '***ensure consistency***' so important? Because inconsistency — showing favoritism to those who violate the compliance program, or don't implement it — undermines the entire idea of compliance, and those responsible for making it happen."

This speaks to institutional justice and institutional fairness. These are not simply the cornerstones of a compliance program — they are the cornerstones of any company. If there is no fairness and justice, what is the point of working for a company? The CCO and compliance function must lead this dialogue in an organization. If the ubiquitous control-overrider and compliance corner-cutter becomes the highest grossing salesperson, receives the biggest bonus and most promotions, this all speaks to a lack of fairness and justice in an organization. It is more than just fairness at the point in time. If such situations exist, employees will correctly conclude that there are no consequences to such action or more insidiously, the only way to get ahead in an organization is to lie, cheat, and steal. This is even more reinforced if the top management actively or tacitly encourages such behavior.

Yet the cost of such a culture is far more than simply the fine or penalty and attendant legal fees incurred. Today, it is far more about the reputational impact. The loss of business is first and foremost, but employees today want to work at ethical companies. The compliance program cannot be seen as simply window dressing. Who would want to work at such a place where, to raise your hand to report unethical and even illegal conduct, meant termination?

The DOJ should be applauded by every compliance practitioner for the 2020 Update. They have reinforced the importance and value of CCOs and corporate compliance programs. The 2020 Update lays out some of the key tools for every compliance professional to utilize.

OneTrust

PRIVACY, SECURITY & GOVERNANCE

About OneTrust

OneTrust is the category-defining enterprise platform to operationalize trust. More than 12,000 customers, including half of the Fortune Global 500, use OneTrust to make trust a competitive differentiator, implementing central agile workflows across Privacy and Data Governance, GRC and Security Assurance, Ethics and Compliance, and ESG and Sustainability. The OneTrust platform is backed by 200 patents and powered by the OneTrust Athena™ AI and robotic automation engine.

In 2020, OneTrust was named the #1 fastest-growing company in America on the **Inc. 500** with a 48,000% three-year growth rate. According to the **IDC Worldwide Data Privacy Management Software Market Shares Report**, 2020, "OneTrust is leading the market outright and showing no signs of slowing down or stopping."

OneTrust has raised a total of $920 million in **funding** at a $5.3 billion valuation from Insight Partners, Coatue, TCV, SoftBank Vision Fund 2, and Franklin Templeton. OneTrust's fast-growing team of 3,000 employees is co-headquartered in Atlanta and London, with offices hubs across Australia, Brazil, Canada, France, Germany, Japan, United Kingdom, and the United States.

To learn more, visit **OneTrust.com** or connect on **LinkedIn**, **Twitter**, and **YouTube.**