



WHITEPAPER

Whistleblowing: How to promote a speak-up culture in your company

What is inevitable: the EU Whistleblower Directive.

What only you can create: a transparent, trustworthy, and legitimate whistleblower system in your organization.

What creates success: analyzing vulnerabilities, developing, and expanding the whistleblower system and training employees.

The new EU Whistleblower Directive sets minimum standards for companies in the European Union in dealing with whistleblowers. Reporting channels must be established, whistleblowers must be better protected, and data protection obligations must be fulfilled. Those who have not yet adapted their policies should do so now, as EU member states



are instructed to transpose the directive into national legislation by the end of 2021.

But even beyond the legal framework, there are good reasons to review and improve the whistleblowing process. A well-functioning system promotes a culture of transparency and values that can save the company from financial and reputational damage.

SAI360 supports compliance managers in optimizing their whistleblower system and offers comprehensive training on whistleblowing. Through interactive training, employees learn when they should make a report and how the system can protect them from retaliation.

HOW COMPANIES BENEFIT FROM WHISTLEBLOWING

We know it's critical to speak up when something is wrong. Whistleblowers are crucial for the preservation of an open and transparent society, as we rely on their courage to expose wrongdoing with their reports. Accessible reporting processes for whistleblowers within a corporate culture are a barometer of morale, and structural deficiencies must be identified before they become a major problem.

- Companies that promote a speak-up culture are perceived as trustworthy and fair by employees, service providers and customers.
- Whistleblowers provide insights into areas that remain hidden in classic feedback channels. They make it possible to stop unlawful activities in companies and avert greater damage with their information.
- Companies where employees frequently interact with the tip system report improved reputation and financial situation.

EU WHISTLEBLOWING DIRECTIVE: WHAT IT SAYS

Until now, whistleblowing has been assessed differently by individual EU states, leading to a lack of adequate protection of whistleblowers against retaliation. Companies and involved authorities had no obligation to establish safe and fair reporting procedures. The EU Whistleblowing Directive adopted in 2019 sets a common minimum standard for the protection of whistleblowers for the first time. The member states must implement it in national legislation by December 2021. Companies can and should aim for higher protections than required by the directive.

THE MAIN PROVISIONS

- A whistleblower system should allow reports to be submitted in writing via an online system, a mailbox or by post or verbally via a hotline. A face-to-face meeting may be scheduled at the whistleblower's request.
- It must be possible to report anonymously as well as by name in all reporting channels. The identity of whistleblowers must be kept confidential.
- Companies must designate an appropriate person to receive and process reports, such as a compliance manager, HR manager or legal counsel. This position can also be held by external individuals. The person who processes incoming reports must be sufficiently trained and familiar with the applicable data protection regulations.
- All indications of violations and unethical behavior must be documented and accessible to authorized individuals. Third parties and the system provider must not have access to sensitive data. Data on whistleblowers and any accused individuals must be processed in compliance with the GDPR
- Whistleblowers must receive an acknowledgement of receipt of the report within seven days. After three months at the latest, they must be informed about the status of the investigation and, if applicable, the results.



- Employees, service providers, suppliers and business partners must be adequately informed about the reporting channels. Multinational companies should provide time and location-independent reporting.
- Whistleblowers must be protected from retaliation in any form. Companies that do not sufficiently protect whistleblowers, or attempt to prevent whistleblowing, must expect penalties.
- The policy encourages whistleblowers to report violations internally first. If they do not have an adequate internal reporting mechanism or if reporting is delayed, they are free to turn to an external body, such as the authorities or the press. Even then, they enjoy whistleblower protection.

These provisions apply to all companies, authorities and organizations with 50 or more employees. Organizations with more than 250 employees must implement the provisions from the end of 2021. Smaller organizations can take advantage of a transition period until 2023.

SEVEN CRITICAL POINTS IN THE WHISTLEBLOWER SYSTEM

The EU Whistleblowing Directive is simply the logical outcome of a realization that compliance managers have come to: Companies need an encouraging, transparent and trust-building whistleblower policy. It is the only way to effectively combat misconduct without damaging corporate culture.

To ensure that everyone can embody the speak-up culture to the fullest, the design of a whistleblower system must include seven central points. Now is the time to take a close look at strategy, eliminate weaknesses and adapt procedures to current requirements. These seven approaches are described here.

1. PRESENT AND ACCESSIBLE REPORTING CHANNELS IMPROVE INDICATIONS

Whistleblowers do not report violations lightly. They often fight the strong urge to remain silent and just let things continue. It is essential to work through several different channels. Accessibility must account for remote work and the home office. Some whistleblowers prefer to express themselves in writing, others verbally or even in person. In addition to a hotline by telephone or recording answering machine, online methods are particularly pivotal. Each channel must be confidential and secure.



It is best practice to integrate whistleblowing into a broader and regularly used feedback system through which employees are already accustomed to sharing their mood, raising minor concerns or asking questions. This way, they are already familiar with the system and have fewer reservations when they make an observation that requires a serious report.

2. DATA SECURITY IS NOT NEGOTIABLE

Compliance management must ensure that data protection is guaranteed throughout the entire reporting process. Processors must be fully trained to keep sensitive information confidential. A data protection breach can not only blow the case but destroy the trust of potential whistleblowers in the whistleblowing system – a far worse outcome.

For security's sake, whistleblowers should be encouraged to disclose only as much information as is necessary to process the report. Investigators should only collect personal data with consent. The duty of care for data security applies to all parties involved.

The providers of whistleblower systems used by a company must not have access to the personnel and case data. It is recommended for European companies to use a provider with server locations in the EU to comply with GDPR regulations in the best possible manner. After retention periods have been met, sensitive data must be reliably deleted.

3. QUICKLY AND THOROUGHLY PROCESSED CASES INCREASE SATISFACTION

Incoming reports from all channels should be managed and evaluated centrally so that relevant parties can compare incidents and identify trends. It is key to provide

sufficient resources when processing reports so that investigators can be well-trained to provide management with concrete and helpful information.

A transparent and expedient case closure increases trust in the whistleblowing process and quickly creates clarity for all parties involved. However, speed must not come at the expense of diligence. Investment in training, personnel and a coherent investigative process structure pays off. Investigators must separate misinformation and defamation disguised as whistleblowing from the truth. Few things damage the whistleblower system more than failed investigations. Mistakes can quickly destroy people's careers and reputations beyond repair.

4. TRANSPARENCY ENCOURAGES WHISTLEBLOWERS

Anyone who notices violations of company guidelines or laws is often unsure how to act. It is therefore imperative to answer all questions about the whistleblowing process transparently, comprehensively and before anyone may need to go through it. This approach gives whistleblowers the orientation and the necessary confidence to initiate the process.

Regular training, information sheets, FAQs and help sections on the whistleblower platforms are key to a workforce empowered to report. The more informed employees are, the more likely they are to seize appropriate opportunities to report. Common questions whistleblowers ask include:

- Is my concern significant enough to be reported?
- Can I submit the report completely anonymously?
- What languages can I report in, and is there a contact person for my preferred language?
- Can I file a report on behalf of a third party who can testify to a violation but does not feel confident to initiate the process themselves?



- Is there a reward for reporting something?
- What protection from retaliation do I have as a whistleblower?
- Do I have to contact an internal body first, or can I make a report to supervisory authorities or the public? Am I then protected as a whistleblower?

- “I don’t want any trouble.”
- “I don’t know if it’s important enough.”
- “I don’t want to inconvenience colleagues.”
- “I could be wrong – what then?”
- “I don’t think my reporting will change anything.”
- “It’s easier if someone else takes care of it.”

5. RETALIATION MUST NOT BE ALLOWED

Whistleblowers can experience an immense variety of reprisals and negative consequences for their report on many levels. They may suddenly be given undesirable tasks, get transferred, experience many forms of social ostracization or even be dismissed. Retaliatory acts are not only ethically wrong and prohibited by law, they also undermine a productive and transparent corporate culture.

Your whistleblowing policy must adequately address retaliation and monitor for the possibility of it occurring at any point throughout any investigation.

The most effective strategy is to sensitize employees permanently and continuously, by frequently communicating to them that retaliation will not be tolerated by the company. This includes placing corresponding anchors in the corporate culture, making commitments in the code of conduct and addressing the matter at staff meetings. Compliance training should make whistleblowing a regular topic. Management needs clear guidance on how to recognize retaliation and prevent it from occurring.

WHAT HOLDS WHISTLEBLOWERS BACK

Reporting a breach takes courage. Here are some of the most cited reasons why potential whistleblowers refrain from reporting. The guidelines and training should address these thoughts and dispel doubts.

6. ACKNOWLEDGING WHISTLEBLOWERS STRENGTHENS THE REPORTING SYSTEM

An internal incident reporting system does not have to mean that positive whistleblowing results remain invisible within the company. Making success visible to employees and management improves trust in the process. Informing employees about the successful work of the reporting system helps to build trust in the processes. Each company needs to decide the level of detail in its reports and that should be clarified by compliance management together with the legal department. Case reports cleansed of sensitive data are also worth considering, as they make the work very tangible and more meaningful.

7. TRAINING CREATES TRUST

A whistleblower system can only be as effective as the people who are supposed to use it.

Every whistleblower system works according to the push principle: it is based on people voluntarily making a report. For it to be well-accepted, the system must be highly visible and lauded by leadership.

Communication campaigns that raise awareness of the system and inform about changes are key tools in effective compliance management. Compliance training on the whistleblower system should take place regularly and focus primarily on the following questions:



- How do I identify incidents where a report is appropriate?
- What should I do if I observe a violation?
- How do I use the reporting system and how does it work?
- How does the reporting system protect my identity and integrity?
- How can I prevent, recognize and act against whistleblowing retaliation?

Training courses must build on each other and reinforce what employees learn, growing confidence steadily over time. When employees feel familiar with the topic and the internal whistleblowing process, you have already made a significant achievement.

A STRONG PARTNER FOR ETHICS & COMPLIANCE TRAINING

SAI360 offers your company a wide range of Ethics & Compliance trainings that educate about whistleblowing and promote a speak-up culture. Each training encourages employees and increases organization-wide confidence in your whistleblowing process.

Our focus is on real-life learning scenarios that motivate participation with a high degree of interaction and hold the learner's attention thanks to captivating problems. The narrated whistleblower scenario is as authentic as possible for a simulation in e-learning. Learners can translate the experience gained in the simulation to real situations with little effort.

Take a look for yourself and try out some of our learning formats. Please **contact us** for a personal demonstration of our online training courses.

About SAI360

SAI360 is the leading ESG cloud provider connecting GRC, EHS, Sustainability and Learning. Our SAI360 platform streamlines workflow and drives outcomes through flexible, scalable, and configurable modules. Our integrated approach sets us apart, helping organizations thrive, create trust, understand their impact, and achieve resilience for over 25 years. SAI360 is headquartered in Chicago, with operations and customers across the globe. Discover more at sai360.com.