» Guide to the Introduction of **Whistleblowing Systems** «

How to successfully implement a whistleblowing system in your organisation – from involving the relevant stakeholders, selecting and setting up the right channels to effectively communicating your whistleblowing system

Index

Introduction

Introducing a whistleblowing system can have economic benefits for organisations of all sizes: employees or other stakeholders represent the first defence against costly misconduct. This early-detection mechanism provides organisations with the opportunity to address concerns at an early stage and prevent financial penalties and reputational damage.

Research consistently demonstrates that hotlines are an effective tool to promote the disclosure of illegal and unethical behaviour. Approximately 90 percent of all whistleblowers try to address their concern internally before going to the authorities, the media or the public – provided they find suitable channels and there is an open speak up culture in the company. Some studies even show that a speak up culture helps companies become more financially successful in the long term.[1]

Whistleblowing is becoming increasingly regulated

Regulation involving whistleblower protection has increased significantly in recent years – and in some countries the establishment of whistleblower channels is already mandatory for companies and government agencies. Below are a few examples:

- In **Germany**, the Money Laundering Act (Geldwäschegesetz) requires, among other things, companies in the financial and real estate sectors to set up anonymous whistleblowing systems.
- In **France**, since 2018, the Sapin II anti-corruption law has obliged all French companies with 50 or more employees to establish a whistleblowing system.
- In the **United Kingdom**, internal whistleblowing has long been standard practice. The FCA, the financial supervisory authority introduced new rules on whistle-blowing in 2016.

[1] Towey, Robert (2018): ***Whistleblowers ultimately help their companies perform better, a new study shows***
Noerr (2017): ***Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie beschlossen***
Les Echos (2018): ***Sapin II : des entreprises très loin de la conformité,***
Handelsblatt (2019): ***EU-Staaten wollen einheitlichen Schutz für Whistleblower***

The largest regulatory initiative is currently taking place at EU level. The **European Union** requires all companies to make secure reporting channels available in the future to whistleblowers and that whistleblowers be entitled to special legal protection.

This guide is intended to help companies create the right conditions to effectively implement and communicate a whistleblowing system within an organisation.

How many reports should companies expect?

The number of reports depends on many variables: company size, organisational structure, sector, jurisdictions, reporting channels and much more. Invariably, the visibility and awareness of the whistleblowing channels has an impact.

According to the Whistleblowing Report 2019, more than 50 percent of companies received whistleblowing reports in 2018. Large companies (more than 250 employees) received an **average of 65 reports**. Smaller companies (20 to 249 employees) received **16 reports**.

Considerations when introducing a whistleblowing channel

When introducing whistleblowing channels for the first time or when reviewing existing whistleblowing arrangements, it's important to consider the broader context in the organisation.

1 Corporate culture

The right corporate culture can be a source of great competitive advantage and speak up culture is key to that. Successful arrangements rely on top-level commitment and messaging, often termed 'Tone from the top', for employees to trust the whistleblowing channels. Does management fully support the system and ensure it is widely communicated?

Along with the full backing of management and the right messaging, organisations must walk the walk. Consider whether employees currently feel comfortable raising concerns, know that their issues will be taken seriously and not fear retaliation. This will indicate whether there is a genuine speak up culture that promotes employee voice.

TIP: Culture surveys can give management an indication of the current status within the organisation and what needs to be worked on and improved.

2 Removing barriers

Employees can be suspicious of whistleblowing arrangements. They may want to know:

- How will you protect my confidentiality/anonymity?
- Will my concern be taken seriously and investigated?
- Will I be retaliated against or potentially lose my job?

This is particularly true when whistleblowing arrangements are first introduced to an organisation.

It is best practice to proactively address these concerns. Communicate that raising a concern helps ensure that the ethical and moral values of the company are upheld. To the best of your ability, be transparent about the speak up process and how the organisation will handle concerns. Emphasise the key role employees play in protecting the organisation against reputational damage and financial loss which is in the interest of all employees.

3 Engaging stakeholders

During the implementation of a whistleblowing system, identify and engage "champions" of the arrangements. These could include the following:

Management

- Proactive communication that top-level management fully supports the introduction of a reporting channel and why („tone from the top").
- Top management should also ensure that all levels of management support the new initiative and understand how to communicate and discuss speaking up and the arrangement with their teams.

The works council/union (for companies this applies to)

- Representatives bodies may have a say in whether a whistleblowing system is introduced and in what form.
- Ensure that the works council/union support the introduction of a whistleblowing system as they can be an important advocate.[2]

[2] Rohde, Silke (2018): *Whistleblowing: So schützen Sie als Betriebsrat Hinweisgeber*

The data protection officer

- The DPO may want to ensure that the workflows around reports and cases are designed and documented in accordance with data protection regulations.

Compliance/HR

- Departments need to work together to define how cases will be managed internally to ensure that they are investigated promptly, and responsibilities are made clear. The department responsible for whistleblowing reports will depend on the organisation so it's important that the arrangements are formalised (see point 4).

IT

- An important stakeholder in the introduction of digital whistleblowing systems.
- The IT team will require relevant documentation/evidence of robust IT security.

Experienced whistleblowing system providers can provide documentation and support to assist with stakeholder engagement.

4 Introducing processes for handling concerns

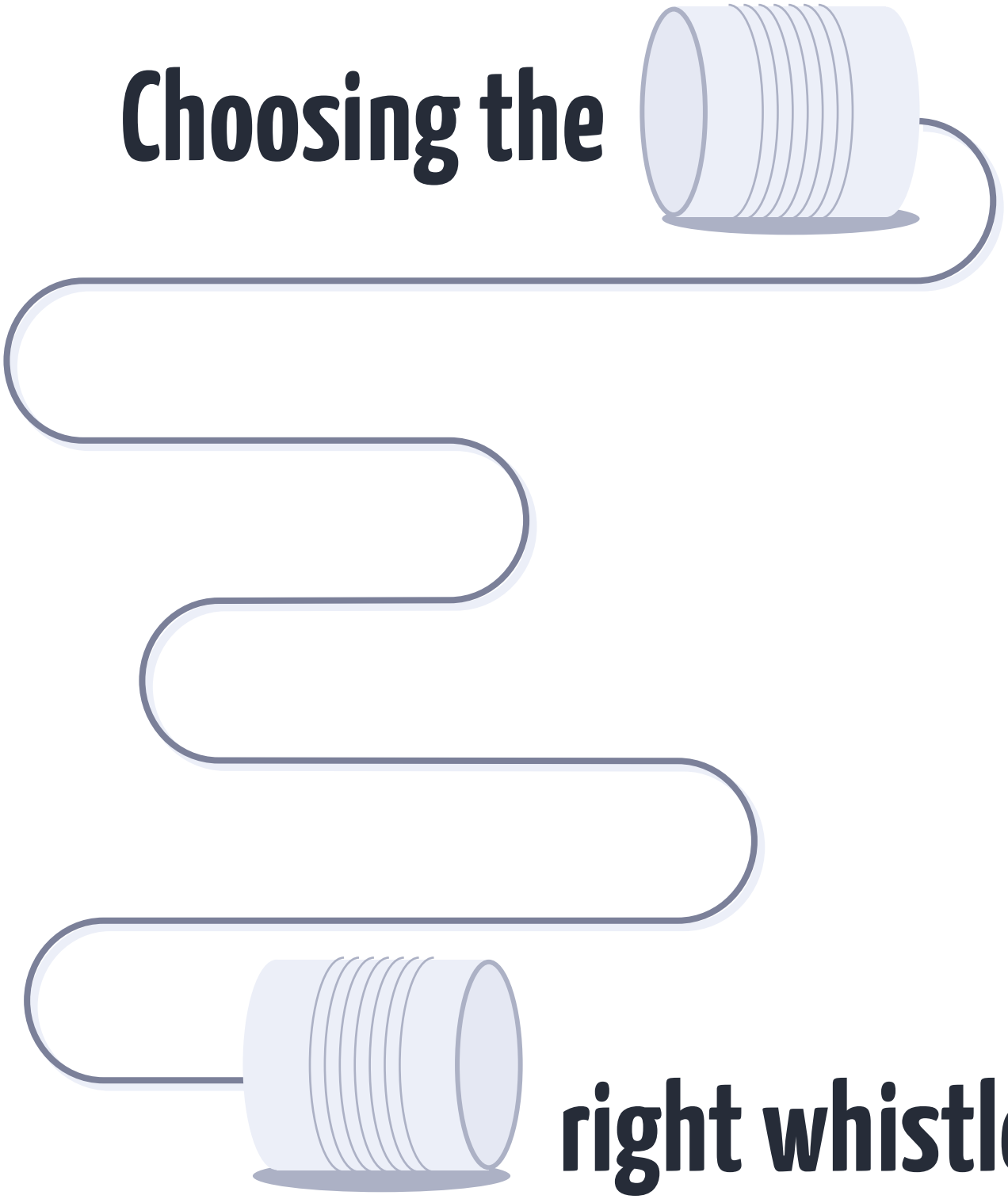
Good systems fail when introduced into bad processes. In advance of the whistleblowing system being implemented, review your triage and investigation processes. This will determine the individuals or teams that handle concerns and how the concerns are investigated.

Some questions that might arise include:

- Should all reports be assessed centrally or automatically routed to the subject matter experts based on the concern?
- What controls are in place to ensure integrity and quality? Should you have approval processes for key actions (i.e. deleting a case)?
- Does the organisation have internal or external subject matter experts it can draw on for investigations?

Organisations with best practice arrangements often have a detailed investigations policy mapping how concerns are handled. This document, if shared with employees, can create greater transparency for potential reporters regarding what happens with their concern.

Choosing the



right whistle-blowing channel

Various channels are available for employees to raise concerns, each offering a unique set of advantages and disadvantages. The most effective approach for organisations is deploying a mixture of channels to increase accessibility and encourage more reports. Below are some areas organisations may wish to take into consideration when choosing their reporting channels.

Defining requirements

Firstly, defining the company's requirements is important. Some questions to consider:

- What are the key issues the company expects to see in reports?
- Which stakeholder groups should be able to submit reports? Will the channel be available to the public via the website?
- Will people submitting a concern be able to do so anonymously?
- Which languages should the whistleblowing system be available in so that it is available to all potential whistleblowers?
- Should the whistleblowing system be available outside normal office or working hours?
- Should the whistleblowing system also be available when employees are on the road or outside the organisation?

Opening the whistleblowing channels to external stakeholders

In a network economy, misconduct and violations of the law can occur not only within the organisation itself, but also within the supply chain or client base. It can serve organisations well to allow external stakeholders to report concerns regarding their employees, suppliers or customers. Their exclusion may represent a missed opportunity to identify misconduct.

While most companies allow customers and suppliers to use their whistleblowing systems, only a fraction of them allow reports from the general public. In countries such as the UK, where internal whistleblowing is more established, twice as many companies allow whistleblowing from the general public as in Germany.

The importance of anonymity

In many countries, protection for whistleblowers is still in its infancy, and potential whistleblowers are often afraid of being retaliated against.

Offering a completely anonymous whistleblower channel is a way of reducing the psychological barrier to raising a concern. According to the Whistleblowing Report 2019, for companies that provide the option of reporting anonymously, 58 percent of initial reports were anonymous. However, one third of these disclosed their identity during the investigation, demonstrating that individuals become more comfortable once trust is established.

Some companies also fear that introducing anonymous reporting could increase the number of abusive reports; studies show, however, that this is not the case. [3]

Promoting dialogue

Often whistleblowers fail to provide all the necessary information in their initial report to allow their concern to be thoroughly investigated. Whistleblowers may also have additional evidence documents to facilitate the investigation or subsequent prosecution.

It is therefore essential that the company is able to communicate with the whistleblower following the initial report.

Advantages and disadvantages of common whistleblowing channels

The most common whistleblowing channels are described here. The table below shows the respective advantages and disadvantages of the various reporting channels.

Postbox: A physical postbox located on the company premises for reports in paper form.

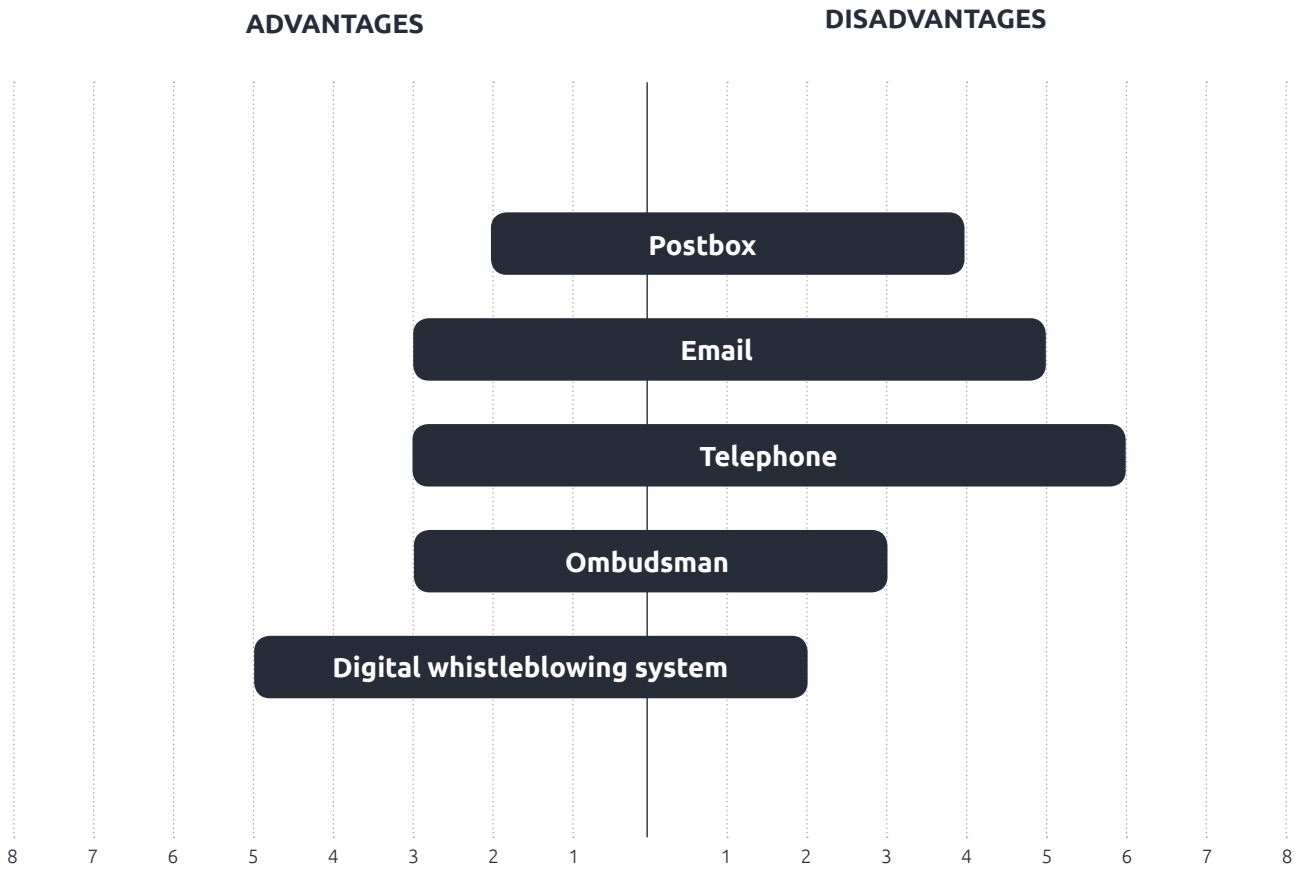
Email: A central email account, such as "compliance@yourcompany.com", to which individuals can send their written concerns.

Telephone: One or more local telephone numbers that enables concerns to be reported. This can be an internal company number or an external call center or answering machine. In the case of the latter, the whistleblower records their message, which is then transcribed and sent to the company.

[3] Prof. Dr. Hauser, Christian et al. (2019): Whistleblowing Report 2019.

Ombudsman: An external independent person, usually a lawyer, who is a contact point for whistleblowers.

Digital whistleblowing system: An online platform where whistleblowers can submit their reports confidentially and anonymously including attachments. The company manages reports using a case management platform which also enables communication with the whistleblower (even if the whistleblower has remained anonymous).



	Pro	Con
Postbox 	■ Available if employees in the company have difficulty accessing other communication channels (internet, telephone). ■ Quick to set up.	■ Whistleblowers have to think carefully about when they post their letter in order to remain anonymous. ■ Handwritten submissions might reveal the identity of the of the whistleblower. ■ Communication with anonymous reporters isn't possible. ■ Not a centralised solution; must be set up and processed separately at each location.
Email 	■ Easy and inexpensive to set up. ■ Reports can be made at any time, globally as well as both internally and externally. ■ Two-way communication with the whistleblower is possible.	■ No anonymity for the whistleblower - emails can always be tracked. ■ No secure transmission of documents. ■ No standard requirements regarding what information should be transmitted by the whistleblower in the message and in which language the message can/should be sent. ■ Laborious, manual management of personal data in accordance with data protection regulations (see GDPR). ■ Risk of email ending up in the wrong hands and compromising confidentiality.
Telephone 	■ Human support for employees often in difficult or emotional situations. ■ Available in any language through an interpretation service. ■ Conversation management approach to gather the relevant information for a report.	■ No anonymity for the whistleblower - even with a secret telephone number, the voice or accent might identify the whistleblower. ■ No means of sending or receiving supporting evidence via the channel. ■ Technical limitations due to legacy technology (sound issues, connectivity, human error). ■ Varying quality and availability of the channel depending on the country or languages. ■ Sensitive internal information shared with external providers. ■ Internal hotlines may not be available 24/7 in any language

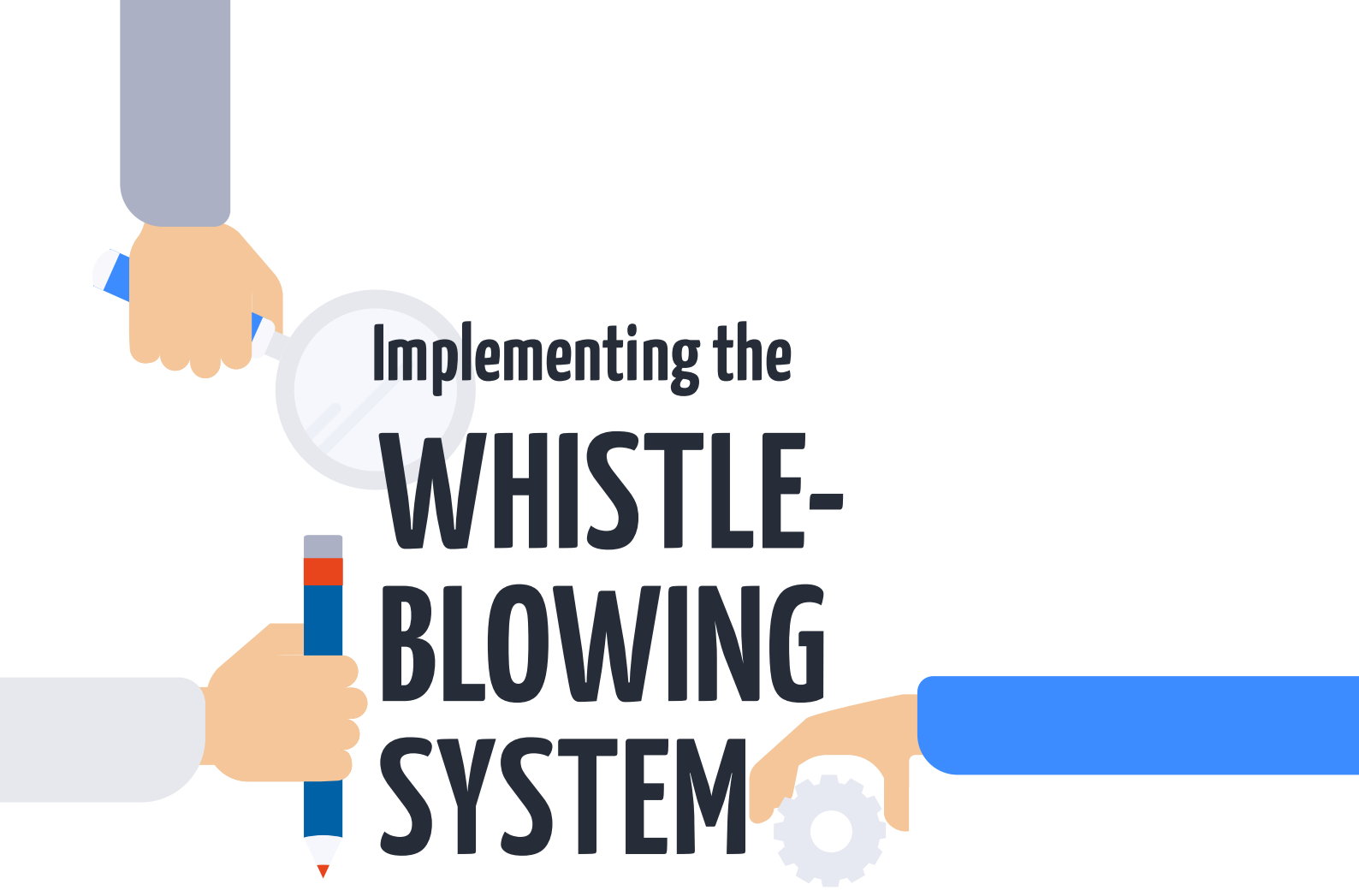
	Pro	Con
External Ombudsman 	■ Legal expertise means the external ombudsman can make relevant enquiries. ■ This channel is external so increases the confidence of potential whistleblowers. ■ If internal resources are lacking, he/she can also take over the assessment and processing of report.	■ No anonymity for the whistleblower if they contact the ombudsman by telephone or email. ■ The time an ombudsman is available and an ombudsman's language skills are generally insufficient for multinational companies. ■ Contrary to public perception, there is no special protection for lawyers operating as independent mediators if the authorities want to search their premises or seize documents.[4]
Digital Whistle-blowing System 	■ Technical measures to ensure anonymity and confidentiality even during follow-up communication. ■ Reporting channel is available globally 24/7 in any language. ■ Accessible on any device (phone, tablet, computer). ■ Secure transfer of files and documents via the internet. ■ Connectivity to a case management tool with automation capabilities (triage, reminders, real-time reporting, workflows).	■ Whistleblower must remember their system login data in order to remain in dialogue with the company. ■ Longer set up time (1-4 weeks).

[4] Prof. Dr. Hauser, Christian et al. (2019): Whistleblowing Report 2019

Our research suggests on average organisations have three reporting channels available to employees[5]. A digital whistleblowing system with specialized reporting channels is now considered best practice for companies[6]. It is scalable making it suitable to both SMEs and large international organisations.

In addition to the dedicated reporting channels described above, employees can raise concerns directly with their line manager or contact the HR or Compliance team. These reports can subsequently be recorded in a digital system to maintain an oversight over all concerns.

[5] Würz, Karl (2018): *Kein Beschlagnahmeverbot bei Rechtsanwälten*
[6] EY (2016): Existing Practice in Compliance 2016. Stand und Trends zum Integritäts- und Compliance-Management in Deutschland, Österreich und der Schweiz.



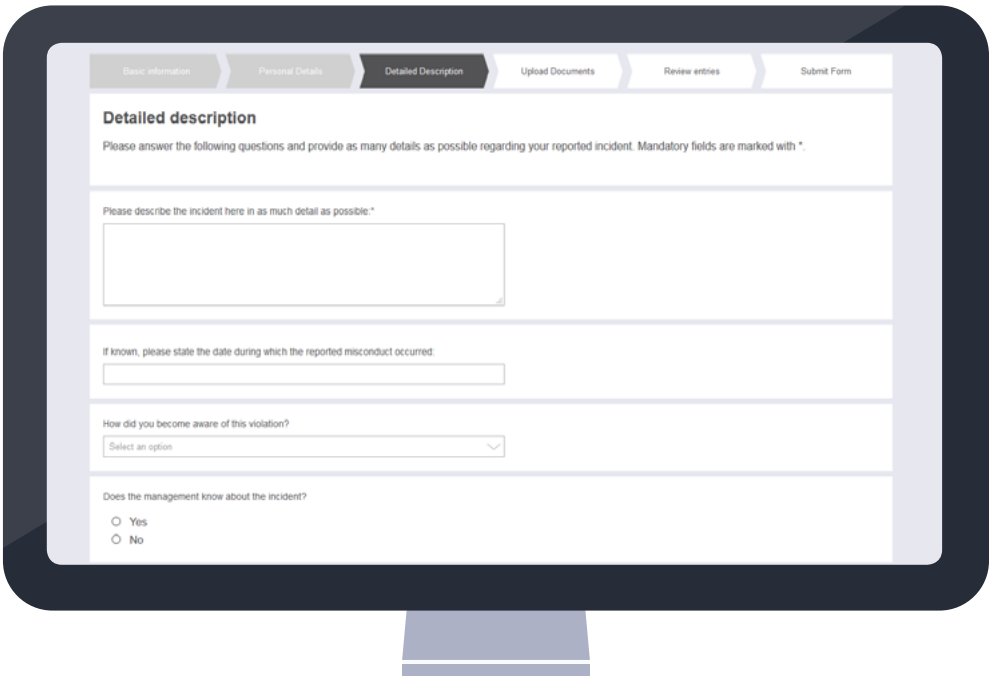
Implementing the WHISTLE-BLOWING SYSTEM

Below are some guidelines on how to implement a digital whistleblowing system.

Draft explanatory text, FAQs and reporting questionnaires

The digital whistleblowing system includes template text that a company can use for explanations, FAQs and the questions that the reporter will need to answer. However, organisations may wish to modify the wording to better reflect their values, branding and tone of voice.

Regarding the length of the reporting questionnaire, it is important strike a balance between gathering sufficient information to conduct an initial assessment of the concern and lengthy questioning making the process cumbersome. Ask the critical questions: Who, What, When, Where, Why, and How?



Don't forget your data protection requirements

Since whistleblower reports often include personal data, companies need to observe data protection regulations when operating a whistleblowing system. Whistleblowing system vendors will usually provide the necessary documents so that the system is compliant in the relevant countries. In addition, law firm Dentons offers a good overview of national data protection requirements in the context of whistleblowing systems. Read more here: *www.whistleblowerguidelines.com*

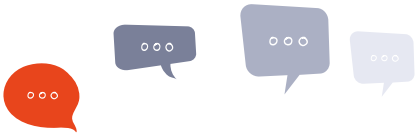
Define reporting categories

With digital whistleblowing systems, employees can select a reporting category. Some examples of possible categories include:

- Bribery, corruption and kickbacks
- Data protection and IT security breaches
- Discrimination, harassment and other labour law problems
- Embezzlement, misappropriation and theft
- Health, safety and environment
- Money laundering
- Tax evasion

Categories are usually based on the types of concerns detailed in the whistleblowing policy. Some organisations restrict the categories to reflect protected disclosures under the legal framework, while others opt for a broader speak up channel that welcomes a variety of concerns to measure the temperature of the organisation.

During implementation, the system will likely provide standard categories that can be modified as required, along with explanations for each category.



Define language and countries

It is possible to integrate any language into a digital whistleblowing system – the text just needs to be translated. As a rule, the system should cover the most important company languages and locations which is often the languages in which the policies and procedures are produced. In some jurisdictions, local legislation may stipulate that employees in that country must have the whistleblowing channel available in the national language.

Define access rights and escalation principles

Who should have access to reports? In a digital system, authorisations can be defined to ensure that any sensitive data is seen on a need-to-know basis. Reminder and alerts may be available to ensure concerns are handled in accordance with you internal KPIs for assigning an investigator, responding to the reporter and concluding the investigation.

Leading whistleblowing programmes have robust approval processes – e.g. the 'four-eyes principle' – that prevent individual users from performing key actions such as deleting a case without authorisation.

Testing the finalised system

After the service provider has set up the system, companies should test whether the messages are routed to the correct place(s), whether the reports are stored correctly in all languages and whether messages are being sent correctly. You may wish to beta test the service on a representative user group to gather feedback about the reporting process before the launch.

Launching the system

If everything is working correctly, the system is ready for launch. The link to the whistleblowing system should be published so that employees have easy access to it, for example on the intranet, in the relevant policies, on the company website, on supplier platforms, in campaigns, on notices or any other location that could help to spread the message.

Care should be taken to ensure that employees can easily access the system.

Communicating the whistleblowing system

Unfortunately, companies regularly neglect this step. The whistleblowing system can only function effectively and reduce risk in the organisation if employees know about it. This requires regular and effective communication.

Getting the message right

Internal whistleblowing is an unfamiliar topic to many employees, and their attention span for compliance issues can be limited.

When communicating the system, companies should therefore note the following:

- The benefits of having a whistleblowing system should be clearly explained. For example, identifying misconduct internally avoids reputational damage and financial loss. This benefits all employees.
- Whistleblowers will not be retaliated against. Where there is reason to believe that misconduct has taken place, the company welcomes concerns being raised (even if they end up being unfounded).
- A concise message needs to make the purpose of the whistleblowing system clear.

Communicate your whistleblowing systems in your company, for example by using flyers and posters.

Involving management is a good idea: a two-minute video with the CEO explaining the purpose of the whistleblowing system demonstrates management support.

Include the overall compliance context

Ideally the communication of the whistleblowing system will be embedded in a larger compliance framework. If this isn't the case, it's possible that employees may get the impression that the company expects compliance violations but is not implementing proactive prevention measures and is not working on an appropriate compliance culture.

Instead it should be made clear that the whistleblowing system is an essential component of the company's overall compliance program. The system should also be mentioned in the Code of Conduct or in the general description of the company's compliance program.

Choose appropriate media and communication channels

There are many ways to promote a whistleblowing system within a company. If the company has a marketing, design or communications department, they might have templates available or can generate ideas.

Examples of communications media:

- Flyers
- Posters
- Newsletters
- Videos
- Banners
- Giveaways

Channels for promoting the whistleblowing system:

- Intranet
- Company website (compliance area)
- Blackboard, video walls, etc.
- Company newsletter
- Staff magazine
- Internal events

The most suitable and effective media and channels will depend on how the company usually communicates internally. Also, the more channels used, the more awareness will be generated.

Repeat communication

Some companies make the mistake of only communicating the system during its introduction. This leads to employees forgetting the system exists and new employees never finding out about it. Over time, the system becomes redundant.

Companies should therefore regularly mention the whistleblowing system when onboarding new employees, for example, or during compliance training. If the company conducts an annual employee survey, they can also ask if employees are aware of the system to bring the system to the forefront of employees' minds.

Some companies also communicate – in anonymous form – reports which have come in and their consequences internally. This is a very transparent way of communicating the benefits of the system to employees and increasing their support for the system.

Conclusion

A well-functioning whistleblowing system is an excellent early warning system to identify risk in a company. The success of the system relies on an open speak up culture where employees do not fear retaliation and know that their concerns will be taken seriously.

It's important that organisations review their arrangements regularly and implement improvements where necessary. Continuing to communicate with employees about the whistleblowing system on a regular basis via several channels to ensure that it remains relevant and continues to be a robust risk mitigation tool is also essential. All of this together ensures that whistleblowing systems continue to play a key role in helping companies avoid sanctions, fines and reputational damage due to misconduct.

Additional resources

Whistleblowing Report 2019

Whitepaper: Reporting Channels

EQS Compliance Blog

About EQS Group

EQS Group is a leading international provider of regulatory technology (RegTech) in the fields of corporate compliance and investor relations. In working with EQS Group, thousands of companies worldwide inspire trust by fulfilling complex national and international disclosure obligations, minimizing risks and communicating transparently with stakeholders.

EQS Group's products are pooled in the cloud-based software EQS COCKPIT. They ensure the professional control of compliance workflows in the fields of whistleblower protection and case management, policy management, insider list management and disclosure obligations.

EQS Group was founded in 2000 in Munich, Germany. Today the group employs more than 400 professionals and has offices in the world's key financial markets.

To learn more, visit us at www.eqs.com or contact us by email at contact@eqs.com.

BEST
DIGITAL
SOLUTIONS

EQS GROUP

www.eqs.com