EU Whistleblower Protection Directive. **Countdown to compliance.**

Our guide to what your organisation can start to do now to prepare for, and gain real value from, the EU Whistleblower Protection Directive.
“After 20+ years working in the field of ethics and compliance, we are delighted to see this law being passed. Whistleblowers are a source of invaluable, hard-to-get information that can potentially save organisations from financial and reputational ruin.”

Karin Henriksson
Founding Partner
karin.henriksson@whistleb.com
+46 70 444 32 16

“Our advice to companies is therefore to do everything they can to support and encourage internal reporting. After all, it is better to deal with a wrongdoing internally, than risk sensitive information ending up in the public domain. It is more important than ever for organisations to offer a secure, user-friendly internal whistleblowing channel.”

Gunilla Hadders
Founding Partner
gunilla.hadders@whistleb.com
+46 70 214 88 73

About WhistleB
WhistleB is a global whistleblowing service provider and business ethics & compliance expert. We help customers to foster a safe and more transparent work environment. The WhistleB system is currently used in more than 150 countries.

Our Story
WhistleB was founded in 2011. From the very beginning, our goal has been to provide a whistleblowing service with industry-leading security and user-friendliness. We are grateful for the confidence that our customers have placed in us, across all continents.
1. Introduction

Why just comply when you can gain real value from whistleblowing?

The EU Whistleblower Protection Directive was approved in April 2019. For the first time, whistleblowers throughout the EU will be protected when they report on breaches of EU law that they become aware of through their workplace.

Most of the organisations affected will now be focused on what needs to be done in order to comply with the Directive by the expected deadline. However, we believe that aiming solely for compliance means that you miss an ideal opportunity for getting real business value from whistleblowing and from the investment you may need to make in a whistleblower system.

For example, many WhistleB customers implement a whistleblowing service as a preventive measure. The very fact that the system is in place prevents misconduct occurring in the first place. Others specifically choose the system because it allows for anonymous reporting and follow-up, thereby increasing the chances of reports being sent. Then there many are customers who implement such a system to show stakeholders that their organisation is committed to building trust doing the right thing.

This guide is aimed to help you both

– comply with the EU Directive on Whistleblower Protection in time.

and

– select, set up and manage a whistleblower channel that delivers real business benefit and protects your long-term success.

Contents

1. Introduction
2. What you need to know about the EU whistleblower directive
3. Your legal obligation to provide a whistleblower channel – how to comply with the directive and excel in whistleblowing
4. ISO 37002 – New global standard on organisational whistleblowing
5. Further information and next steps
2. What you need to know about the EU Whistleblower Protection Directive

What is the purpose of the Directive?
The EU Whistleblower Protection Directive aims to protect whistleblowers throughout the EU who report on a range of misconduct that they become aware of through their workplace, and encourage more people to dare to blow the whistle.

Which organisations are affected?
The Directive states that all private legal entities with 50 or more employees will need to establish secure reporting channels. Additionally, companies operating in specific areas such as financial services, products and markets and companies that are vulnerable to money laundering or terrorist financing will also need to comply. All public legal entities will also need to comply, with some potential exceptions for smaller municipalities and public entities.

Through which channels can whistleblowers report and remain protected?
According to the Directive, employees are to be encouraged to report internally first to their employer if a functioning internal channel is available to them. However, whistleblowers will be able to select the most appropriate channels for the circumstances of their case, without losing the protection granted by the EU Whistleblowing Directive, this includes reporting externally to competent national or EU authorities or to the media.

What kind of internal channel needs to be implemented?
The EU Whistleblower Protection Directive places specific requirements on the nature of the whistleblowing channel to be provided. It details requirements regarding:

1. Confidentiality of the identity of the whistleblower
2. Response times
3. Contact persons
4. Follow-up
5. Communication
6. GDPR compliance
7. Record keeping
(See more details on each requirement in section 3.)

What can whistleblowers report on?
Whistleblowers will be able to sound the alarm on a range of issues and remain protected from recrimination when they do so. Issues include anti-money laundering and corporate taxation, data protection, protection of the Union’s financial interests, food and product safety and environmental protection and nuclear safety.

Who can report?
Everybody who works in the private or public sector. The EU Whistleblower Protection Directive applies to employees, self-employed people, freelancers, consultants, contractors, suppliers, volunteers, unpaid trainees and job applicants, who acquire information on illegal activities in a work-related context. It also covers those who support whistleblowers such as family members and colleagues.
What if my organisation fails to comply?

The EU Whistleblower Protection Directive requires penalties against those who attempt to hinder reporting, retaliate against whistleblowers, attempt to bring proceedings or who reveal the identity of the whistleblower. Any threats or attempts to retaliate against whistleblowers are also prohibited.

What is the timing for compliance?

16th April 2019
Approval of the EU Whistleblower Protection Directive by the European Parliament, after which the new law is to be approved by EU ministers.

Second half of 2021
(or two years after adoption) The new law must be embedded into national law by the Member States. Organisations with 250 employees or more must be ready to comply with the new law.

Second half of 2023
(or two years after the law comes into force) Legal entities with 50 – 249 employees must be ready to comply with the new law.
3. Your legal obligation to provide a whistleblower channel
– how to comply with the directive AND excel in whistleblowing

All companies with 50 or more employees will be required to establish secure reporting channels according to specific requirements. We have broken down these requirements and provide our advice below:

1. Confidentiality of the identity of the whistleblower

| What the law says | The procedures for reporting and following-up of reports shall include channels for receiving the reports which are designed, set up and operated in a secure manner that ensures the confidentiality of the identity of the reporting person and any third party mentioned in the report, and prevents access to non-authorised staff members. |
| WhistleB advice | Allow anonymous reporting and dialogue  
- Anonymous reporting and dialogue are essential for people to dare to reach out. Use a system that enables you to ensure the whistleblower’s anonymity both when reporting and in the following dialogue.  
- Use a system with a secure Case management tool, through which you can appoint people who are authorised to read and act on reports received. |

2. Response times

| What the law says | The procedures for reporting and following-up of reports shall include an acknowledgment of receipt of the report to the reporting person within no more than seven days of that receipt. |
| WhistleB advice | Be responsive to build trust  
- Make sure that the whistleblower instantly receives confirmation that the message has been received, for example via an on-screen message.  
- The receiver of whistleblower messages should be notified immediately by text message and e-mail that a report has been received. However, limit use of e-mail to notifications, all whistleblower messages that can contain sensitive or personal data should be securely encrypted and managed within a secure system.  
- Make sure that you have a dedicated team to receive the reports, and the right team to handle and answer them.  
- If your organisation receives many messages, you might want to have standard messages ready to send out to the whistleblower. |
3. Contact persons

<table>
<thead>
<tr>
<th>What the law says</th>
<th>The procedures for reporting and following-up of reports shall include the designation of an impartial person or department competent for following up on the reports (...) and which will maintain communication with and, where necessary, ask for further information from and provide feedback to the reporting person.</th>
</tr>
</thead>
</table>
| WhistleB advice | **Ensure the right system, skills and routines are in place to handle investigations**
- Set up a team that is as non-operational as possible, and with roles from a range of different parts of the organisation. This strengthens the integrity of the team. In the WhistleB 2019 customer study on organisational whistleblowing, the whistleblowing team most often included these competences: legal and compliance, internal audit and risk, ethics and HR. Having Board representatives on the team is also becoming more common.
- Make sure that you have a system that allows you to add the competences you need per case.
- Make sure that you have an easy-to-use channel through which the whistleblower can add pictures, videos, text documents and other file formats while also allowing metadata cleansing. |

4. Follow-up

<table>
<thead>
<tr>
<th>What the law says</th>
<th>The procedures for reporting and following-up of reports shall include diligent follow-up to the report by the designated person or department, diligent follow up where provided for in national law as regards anonymous reporting, and a reasonable timeframe to provide feedback to the reporting person about the follow-up to the report.</th>
</tr>
</thead>
</table>
| WhistleB advice | **Select a robust case management system to underpin diligent follow-up**
- Ensure your whistleblower system includes a case management tool that is integrated with the reporting channel and allows for dialogue with an anonymous or non-anonymous whistleblower. This will ensure seamless, compliant and secure case follow-up and processing. According to WhistleB’s 2019 customer study on organisational whistleblowing, approximately 50 % of all reports lead to a dialogue with the whistleblower.
- If your organisation operates multi-nationally, select a system with safe translation support for communication in any language. |
| | **Assess how your organisation handles investigations**
- Treat investigations with the utmost confidentiality and with respect for both the whistleblower and the person accused.
- Establish processes for any action plans needed based on the outcome of the investigations.
- Investigations can require very specialist skills which leaders may need to source externally, or you might want to have an external team to receive your reports. In this case, a system that allows external users to be securely included in case handling is important. |
## 5. Communication & information

<table>
<thead>
<tr>
<th>What the law says</th>
<th>WhistleB advice</th>
</tr>
</thead>
<tbody>
<tr>
<td>The procedures for reporting and following-up of reports shall include clear and easily accessible information regarding the conditions and procedures for reporting externally to competent authorities and, where relevant, to institutions, bodies, offices or agencies of the Union.</td>
<td>Do all you can to give people confidence to report internally</td>
</tr>
<tr>
<td></td>
<td>A GDPR compliant system makes things easy for you</td>
</tr>
<tr>
<td></td>
<td>✓ Choose a system that is GDPR compliant, already built to help you to comply with the GDPR.</td>
</tr>
<tr>
<td></td>
<td>✓ Useful features for compliance include case and user logs, safe translations and deletion of personal data when the case is closed.</td>
</tr>
<tr>
<td></td>
<td>✓ Check that you inform potential users correctly about national differences in reporting.</td>
</tr>
</tbody>
</table>

Having your own trustworthy whistleblowing system, knowledgeable people handling the messages and a thorough process increase the organisation’s chances of receiving messages internally. Reports received through internal channels give leaders the opportunity to address and correct matters appropriately internally before information ends up in the public domain. To further reduce the barriers to internal reporting, select a system that is easy to use and available 24/7 from a range of devices.

A robust whistleblowing system is a concrete way of showing that you mean what you say in your ethical guidelines and that the organisation is willing to listen when things go wrong. It is also a form of insurance; with an internal whistleblowing system in place you can prevent inappropriate conduct happening in the first place.

## 6. GDPR Compliance

<table>
<thead>
<tr>
<th>What the law says</th>
<th>WhistleB advice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any processing of personal data carried out pursuant to the Directive must comply with the GDPR.</td>
<td>A GDPR compliant system makes things easy for you</td>
</tr>
<tr>
<td></td>
<td>✓ Choose a system that is GDPR compliant, already built to help you to comply with the GDPR.</td>
</tr>
<tr>
<td></td>
<td>✓ Useful features for compliance include case and user logs, safe translations and deletion of personal data when the case is closed.</td>
</tr>
<tr>
<td></td>
<td>✓ Check that you inform potential users correctly about national differences in reporting.</td>
</tr>
</tbody>
</table>

## 7. Record keeping of the reports

<table>
<thead>
<tr>
<th>What the law says</th>
<th>WhistleB advice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorities, private and public legal entities must keep records of every report received, in compliance with the confidentiality requirements provided for. Reports shall be stored for no longer than it is necessary and proportionate.</td>
<td>Complete and close cases within one integrated whistleblower system</td>
</tr>
<tr>
<td></td>
<td>✓ Ensure that you can keep a user and case log of each case. A GDPR compliant whistleblowing system does this automatically for you.</td>
</tr>
<tr>
<td></td>
<td>✓ Ensure that your whistleblowing system allows for deleting personal data in line with the GDPR principle of accountability.</td>
</tr>
</tbody>
</table>
In addition to the above specific requirements the EU Whistleblower Protection Directive places on organisations, we also recommend organisations to consider the following as part of their whistleblowing system review.

1. **Update associated policies and training**

The new EU Whistleblower Protection Directive requires that penalties be imposed for retaliation against whistleblowers. It is therefore a good idea to review your Code of Conduct to ensure that it details behaviour that could be defined as “retaliation” and explains that it is neither tolerated nor legal. Training related to the organisation’s code of conduct and whistleblowing should also be updated in line with the new directive.

2. **Foster the right culture**

As we’ve mentioned above, once the EU directive protects a whistleblower who may report externally, it is critical to encourage internal reporting as far as possible. Communication is a fundamental element in this. Show your employees and others that your organisation is open to whistleblowing, that it values whistleblowing information, and that leaders are committed to listen to and to act on reports received.
4. ISO 37002 – New global standard on organisational whistleblowing

Whether organisations fall under the scope of the EU Whistleblower Protection Directive or not, practical guidance on whistleblowing management is always valuable. The new global standard for organisational whistleblowing currently being developed by the ISO comes at the right time. ISO 37002 will provide practical guidance to organisations on a broad array of whistleblowing management aspects. It doesn’t specify requirements but provides guidance on whistleblowing management systems and recommended practices.

ISO 37002 is scheduled for completion by the end of 2021, the time when the EU Directive is expected to come into force. It is intended to provide guidelines for implementing, managing, evaluating, maintaining and improving a robust and effective management system for whistleblowing within an organisation.

The international standard aims to guide organisations in managing the full cycle of whistleblowing:

- Identification and reporting of concerns of wrongdoing
- Assessment of concerns of wrongdoing
- Means of addressing concerns of wrongdoing
- Closing of whistleblowing cases

WhistleB is part of and contributes to the working group developing and drafting the standard.
5. Further information and next steps towards your countdown to compliance

WhistleB is ready to help your organisation prepare to comply with the EU Whistleblower Protection Directive and we can help you with all the tips mentioned above. We have a leading, secure digital whistleblower system used by hundreds of organisations worldwide, and over 25 years of experience in compliance and ethics. We stay ahead of the latest laws and embed compliance into effective solutions that fit your organisation’s unique demands.

Contact us if you would like a free consultation on your readiness for compliance with the EU Whistleblower Protection Directive:

info@whistleb.com

You can follow the latest developments on how the Directive is implemented as national law on WhistleB’s Resource Centre for the new law: https://whistleb.com/eu-whistleblower-protection-directive/
WhistleB provides a whistleblowing service for companies, authorities and organisations. Our solutions are used in more than 150 countries. WhistleB has more than 25 years of experience in the fields of compliance and corporate sustainability. We are committed to helping customers minimise their risks and strengthen their performance through high ethical procedures and a leading whistleblowing service.

For more information about this study, or if you have further questions concerning corporate whistleblowing, please contact Karin Henriksson, Co-founder of WhistleB, karin.henriksson@whistleb.com.