WhistleB’s best advice on how to comply with the EU Whistleblower Protection Directive

Organisations will be obliged to establish internal 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

<table>
<thead>
<tr>
<th>What the law says</th>
<th>Allow anonymous reporting and dialogue</th>
</tr>
</thead>
</table>
| 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. | **✓** 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. |

© WHISTLEB WHISTLEBLOWING CENTRE 2019

info@whistleb.com  www.whistleb.com
## 2. Response times

<table>
<thead>
<tr>
<th>What the law says</th>
<th>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.</th>
</tr>
</thead>
</table>
| 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, 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 a 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: approximately 50% of all reports lead to a dialogue with the whistleblower.  
✓ If your organisation operates multinationally, 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>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.</th>
</tr>
</thead>
</table>
| WhistleB advice | **Do all you can to give people confidence to report internally**  
Having your own trustworthy whistleblowing system, knowledgeable people handling the messages and a thorough process increase the organisation’s chances of receiving messages internally, and to be able to address and correct matters appropriately. 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>Any processing of personal data carried out pursuant to the Directive must comply with the GDPR.</th>
</tr>
</thead>
</table>
| WhistleB advice   | A GDPR compliant system makes things easy for you  
✓ Choose a system that is GDPR compliant, built to help you to comply with the GDPR.  
✓ Useful features for compliance include case and user logs, safe translations and deletion of personal data when the case is closed.  
✓ Check that you inform potential users correctly about national differences in reporting. |

7. Record keeping of the reports

<table>
<thead>
<tr>
<th>What the law says</th>
<th>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.</th>
</tr>
</thead>
</table>
| WhistleB advice   | Complete and close cases within one integrated whistleblower system  
✓ Ensure that you can keep a user and case log of each case. A GDPR compliant whistleblowing system does this automatically for you.  
✓ Ensure that your whistleblowing system allows for deleting personal data in line with the GDPR principle of accountability. |

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.

For more information about this study, or if you have further questions concerning corporate whistleblowing, please contact:

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