Case IQ

How Case IQ Helps You Go Above and Beyond EU Whistleblower Directive Requirements

During an investigation under the EU Whistleblower Directive, organizations are required to follow specific procedures to ensure compliance and transparency while protecting the whistleblower. Here are the various requirements under the WBD, and how Case IQ can help you go above and beyond to reduce risk and encourage greater transparency:

EU Whistleblower Directive Requirement	How Case IQ Helps You Go Beyond
ESTABLISHMENT OF SECURE INTERNAL REPORTING CHANNELS: Organizations must set up secure, confidential channels for whistleblowers to report breaches. These channels can include email, phone lines, or web portals. The setup must ensure: • Confidentiality of the whistleblower's identity. • Proper recording of all reports, ensuring that each report is documented with the necessary details, including the nature of the breach, the timeline, and any evidence provided. • Acknowledgment of the report within seven days of receipt, confirming that the whistleblower's complaint has been received.	Case IQ offers multiple secure internal reporting channels to encourage an unbiased speak up culture. Confidential and secure reporting is available through email, webform, telephone hotline, all with anonymity built right in. Automatic email notifications are sent to ensure organizations are made aware of new reports and ensure they acknowledge the receipt of the complaint.
INVESTIGATION PROCESS: Once a report is submitted, the following activities and documentation are necessary: • Initial Assessment: The organization should document the initial assessment to determine the credibility and seriousness of the claim. This involves reviewing the report and determining whether the matter requires a full investigation. • Appointment of an Investigation Team: The investigation must be carried out by a neutral and independent team within the organization, or sometimes externally, depending on the nature of the report. Documentation should include the selection process of investigators, ensuring they do not have conflicts of interest. • Interviews and Evidence Collection: The investigation team must document all interviews, meetings, and evidence collected, including testimony from the whistleblower and other involved parties. All findings must be written in clear, detailed records. • Legal Compliance Check: Organizations must assess the breach in light of applicable EU and national laws. Documentation should include references to the relevant laws and regulations that apply to the alleged misconduct (e.g., GDPR, environmental regulations, anti-corruption laws).	Case IQ's purpose-built and configurable workflows ensure that the organization can build out processes and have a centralized repository to outline and define the initial assessment, and appointment of investigative team. Case IQ's form builder allows for organizations to capture all related interview and evidence in a secure and centralized location. Case IQ's enterprise-wide collaboration features allow for organizations to seamlessly include collaborators to a case file for legal compliance check.
WHISTLEBLOWER PROTECTION: • Non-Retaliation Measures: The organization must ensure the whistleblower is protected from retaliation. This includes documenting any steps taken to shield the whistleblower from	Case IQ's anonymous reporting ensures that reporters will remain anonymous from the investigative team.

demotion, dismissal, or harassment. If any action is taken against the whistleblower, documentation of these actions must be thorough, providing evidence that the action is unrelated to the whistleblower's complaint.

- Regular Follow-Up: The organization must provide updates to the whistleblower within three months. Documentation should include all communications between the organization and the whistleblower, ensuring transparency in the investigation's progress.

Case IQ's configurable workflow and notification rules mitigate the risk of follow-ups or tasks slipping through the cracks and ending in non-compliance.

FINAL REPORT AND OUTCOME:

- Findings and Conclusion: At the end of the investigation, a comprehensive report is created, detailing all findings, decisions made, and actions taken (or not taken). This final report includes:
  - A summary of the investigation process.
  - Evidence supporting the findings.
  - The outcome, including whether the allegations were substantiated or not.
  - Any corrective actions taken (e.g., disciplinary action, policy changes, legal reporting).
- Remediation Plan: If the complaint is valid, the organization may need to take corrective actions such as implementing new internal controls, policies, or compliance training programs. Documentation of these plans should be part of the final investigation file.

Case IQ's template generator allows organizations to upload existing investigative templates into their Case IQ application.

Organizations can leverage the Case IQ system as their single source of truth by having the application auto-populate templates in a single click of a button.

Case IQ's AI Summarization Pilot goes one step further and generates an Investigative Summary which is exportable from the case file.

Remediation plans, corrective actions, and prevention opportunities can be defined and documented within Case IQ and included in the generated summaries.

REPORTING TO AUTHORITIES:

In some cases, organizations may be legally required to report findings to external authorities (such as regulatory bodies or law enforcement). Documentation must show compliance with these legal obligations, including copies of all reports submitted and correspondence with authorities.

Case IQ allows you to seamlessly export case files and evidence to external authorities.

All activities within a case file are time stamped and dated within a case file audit trail.

RECORD-KEEPING:

All documents related to the whistleblower case, including the original report, investigation notes, evidence, internal communications, and final conclusions, must be securely stored for future reference. The organization is required to keep these records confidential but accessible for audits or in case of further legal actions.

Case IQ's world-class analytics platform built into the application allow organizations to identify trends, problem areas, and preventative opportunities.

With Case IQ's partnership with Microsoft Azure, SOC2, HIPAA, and GDPR compliance, we can ensure the sensitive data and records being stored within the application are secure at all times.

In conclusion, organizations must ensure detailed and secure documentation of all activities related to whistleblower reports. These reports must follow the EU Whistleblower Directive's guidelines to protect whistleblowers and comply with legal requirements. Regular audits and checks should be in place to ensure ongoing compliance with these directives. Case IQ gives organizations the perfect system to not only comply with these current requirements with ease, but also to adapt to new regulations as they evolve.