THOMSON REUTERS
PRACTICAL LAW™

Whistleblower Programs and EU Data Protection Law Compliance: Overview

by Alja Poler De Zwart, Partner, Morriston & Foerster, with Practical Law Data Privacy Advisor

Status: **Maintained** | Jurisdiction: **European Union**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-020-0857**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

A Practice Note providing an overview of issues relating to whistleblowing programs and data protection law compliance in the EU. This Note discusses the legal framework governing whistleblowing programs in the EU and provides an overview of the EU Whistleblowing Directive's requirements (Directive (EU) 2019/1937 on the Protection of Persons Who Report Breaches of Union Law). This Note also provides an overview of key data protection law considerations under the EU General Data Protection Regulation (GDPR) in the context of whistleblowing programs, such as data subject notice requirements and data subject rights.

An increasing global focus on compliance and various legal requirements have led organizations to establish whistleblower hotlines or programs that protect employees and other parties reporting misconduct in the workplace. Whistleblowing programs enable organizations to learn about, investigate, and remedy conduct that:

- Exposes the organization to civil or criminal liability, such as:
  - anticompetitive activities;
  - financial or tax fraud;
  - bribery;
  - environmental damage;
  - poor labor standards;
  - unsafe products or services; and
  - discrimination and harassment.
- Violates the organization's codes of conduct or employee policies and procedures.

In the EU, Directive (EU) 2019/1937 on the Protection of Persons Who Report Breaches of Union Law (Whistleblowing Directive) requires certain organizations to implement whistleblower protection programs and sets out the minimum standards for these programs. EU member states must implement the Whistleblowing Directive into their national laws by December 17, 2021. This Note discusses:

- The legal framework governing whistleblower programs in the EU.
- The Whistleblowing Directive's requirements.
- Complying with the GDPR when operating a whistleblower program.

Employment and labor code requirements and employee privacy issues that arise during the investigation and adjudication of whistleblower retaliation complaints are outside the scope of this Note.

For information on operating whistleblower programs outside the EU, see Practice Notes, Whistleblower Hotlines and Non-US Data Protection Law Requirements: Overview and Whistleblower protection.

Legal Framework Governing Whistleblowing Programs

Whistleblower Protection Laws and Whistleblowing Directive

On December 16, 2019, the Whistleblowing Directive entered into force. It sets new EU-wide minimum standards for protecting whistleblowers and requires EU member states to establish comprehensive whistleblower protection frameworks. The Whistleblowing Directive addresses:

- Procedures for establishing internal and external reporting channels for receiving and investigating complaints relating to potential violations of a broad range of EU laws.
- The scope of activities that whistleblowers may report.

- Protections for whistleblowers.
- Examples of retaliation that trigger whistleblower protection.

EU member states must transpose the Whistleblowing Directive into their national laws by December 17, 2021, at which time organizations with at least 250 workers must comply. However, private sector organizations with 50 to 249 workers have until December 17, 2023 to comply with the Whistleblowing Directive's internal reporting channel requirements in Article 8(3) (Article 26(1), (2), Whistleblowing Directive; see Applicability of Whistleblowing Directive).

The Whistleblowing Directive establishes the minimum standards required in EU member state implementing laws and permits EU member states to customize their laws, for example, by determining what penalties apply for violations and expanding the scope of reportable concerns. This will result in different whistleblowing program requirements throughout the EU. Organizations must understand which EU member state laws apply to them and monitor their implementation and related supervisory authority guidance.

A minority of EU member states enacted comprehensive whistleblower laws before the Whistleblowing Directive, including France, Malta, Hungary, Ireland, Italy, Lithuania, the Netherlands, Slovakia, and Sweden. Other EU member states have whistleblower protection laws that apply only to public servants or specific sectors, such as financial services.

EU member states may revise existing whistleblower protection laws or pass new laws implementing the Whistleblowing Directive. As of the date of this Note, Denmark and Sweden are the only member states that have implemented the Whistleblowing Directive into their national law, though most member states have begun the legislative process. For more on the status of EU member states' implementing laws, see Morrison & Foerster, Whistleblowing Resource Center: Local Implementation. The details of EU member states' implementing laws are outside the scope of this Note.

Iceland, Liechtenstein, and Norway are still debating how to incorporate the Whistleblowing Directive into the European Economic Area (EEA) Agreement.

GDPR and National Data Protection Laws

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) also has implications for processing personal data in the context of whistleblowing programs. The GDPR replaced the EU Data Protection Directive (Directive 95/46/EC) (EU Directive) as of May 25, 2018 and introduced a single data protection framework across the EU. The EEA Joint Committee incorporated the GDPR into the EEA Agreement on July 6, 2018, extending the GDPR's application to Iceland, Liechtenstein, and Norway.

The GDPR includes several provisions allowing EU member states to enact national legislation specifying, restricting, or expanding some requirements. All EU member states have enacted national laws implementing the GDPR, except for Slovenia (see Article, National Implementation of the GDPR). EU member state supervisory authorities may also issue guidance on the topic of whistleblowing programs in addition to their implementing laws, as they did for the GDPR (see Practice Note, GDPR Data Protection Authority Guidance Tracker by Country (EEA)).

Organizations subject to the GDPR must therefore comply with both the GDPR and any applicable national data protection laws when operating whistleblower protection programs. For more information on the applicability of the GDPR, see Practice Note, Determining the Applicability of the GDPR. For more information on national laws implementing the GDPR, see GDPR National Implementation Legislation Toolkit.

Whistleblowing Directive Requirements and Restrictions

The Whistleblowing Directive requires covered organizations to implement whistleblowing programs that enable individuals to report a wide range of EU law violations. It sets minimum standards for organizations on how to establish reporting channels and respond to and address whistleblower reports.

Applicability of Whistleblowing Directive

The Whistleblowing Directive requires organizations with more than 50 workers to set up a whistleblowing program (Article 8(3), Whistleblowing Directive). Workers are individuals who, for a certain period of time, perform services for and under the direction of another person for remuneration, including:

- Full-time employees.
- Part-time employees.
- Trainees.
- Interns.
- Fixed-term contract workers.

(Recital 38, Whistleblowing Directive.)

The Whistleblowing Directive does not state whether an organization's 50 workers must be physically located in the EU, but EU member states may clarify this in

their implementing laws. However, it is highly likely that the Whistleblowing Directive will apply to non-EU entities that employ more than 50 workers located in the EU, considering that European labor law applies to employees located in the EU regardless of their employer's location.

The Whistleblowing Directive also states that EU member states may encourage organizations in the private sector with fewer than 50 workers to establish internal reporting channels (Recital 49, Whistleblowing Directive). It is unclear whether this will result in legal requirements for these organizations or voluntary implementations of whistleblowing programs (Article 8(7), Whistleblowing Directive).

Reportable Concerns

Whistleblowers may report concerns under the Whistleblowing Directive for violations of EU law in the areas of:

- Public procurement.
- Financial services.
- Products and markets.
- The prevention of money laundering and terrorist financing.
- Product safety and compliance.
- Transport safety.
- Protection of the environment.
- Radiation protection and nuclear safety.
- Food safety, animal health, and welfare.
- Public health.
- Consumer protection.
- Protection of privacy and personal data and security of network and information systems.
- Breaches of the EU's financial interests.
- Breaches related to the EU internal market (including state aid rules and corporate tax rules).

(Article 2(1) and Recital 19, Whistleblowing Directive.)

The Whistleblowing Directive permits member states to expand the scope of reportable concerns in their implementing laws to:

- Ensure comprehensive whistleblower protection frameworks at a national level.
- Prevent underreporting by whistleblowers.
- Strengthen enforcement of applicable law.

(Article 2(2) and Recitals 5 and 24, Whistleblowing Directive.)

The European Commission also issued a statement encouraging EU member states to extend the Whistleblowing Directive's scope of application to other areas in their implementing laws.

Protected Individuals

The Whistleblowing Directive's protections apply broadly to all whistleblowers in the private and public sector who acquire information on EU law breaches in a work-related context. This may include:

- Current and former employees.
- Shareholders.
- Interns.
- Job applicants.
- Trainees.
- Contractors and subcontractors.
- Volunteers.
- Suppliers.
- Facilitators, colleagues, or relatives of the whistleblower who have a work-related connection to the whistleblower's employer, customer, or recipient of services.

(Article 4 and Recitals 37 to 41 and 55, Whistleblowing Directive.)

Reasonable Grounds for Reporting

Whistleblowers must have reasonable grounds to believe that the concern they report is true in light of the circumstances and the information available to them when they report (Article 6(1) and Recital 32, Whistleblowing Directive). The Whistleblowing Directive does not provide any additional guidance or examples of what constitutes reasonable grounds, though future regulatory guidance may clarify this.

The Whistleblowing Directive protects whistleblowers regardless of their motives for reporting a violation (Recital 32, Whistleblowing Directive). EU member state implementing laws must include penalties for whistleblowers who knowingly report or publicly disclose false information and measures to compensate those damaged by a false report (Article 23(2) and Recitals 101 and 102, Whistleblowing Directive).

Anonymous Reporting

The Whistleblowing Directive permits EU member state laws to address whether organizations and authorities must accept and respond to anonymous reports. However, the Whistleblower Directive's protections will still apply to whistleblowers who:

- Make a report or a public disclosure anonymously.
- Have reasonable grounds to believe that the concern they report is true in light of the circumstances and the information available to them when they report.
- Are subsequently identified.
- Experience retaliation regarding the report or disclosure.

(Article 6(2), (3) and Recital 34, Whistleblowing Directive.)

Reporting Channels

The Whistleblowing Directive establishes three channels for whistleblowers to report their concerns. These three channels are:

- Internal reporting within their organization (see Internal Reporting).
- External reporting to national and EU authorities (see Reporting to EU and Member State Authorities).
- Public reporting and disclosures (see Public Reporting).

Organizations must provide clear and easily accessible information on the procedures for reporting concerns:

- Within the organization.
- Externally to EU or member state authorities.
- To EU institutions, bodies, offices, or agencies, when relevant.

Organizations should post this information in a prominent location accessible to all workers and on their website and include it in ethics and compliance training (Article 9(1)(g) and Recital 59, Whistleblowing Directive).

Internal Reporting

The Whistleblowing Directive encourages whistleblowers to first report their concerns through internal channels when the organization can address the report internally and there is no risk of retaliation (Article 7(2) and Recital 47, Whistleblowing Directive). Organizations may decide what reporting channels to establish if they enable individuals to submit confidential and secure reports in writing, orally, or through both methods. The Whistleblowing Directive sets out the several options, including:

- By post.
- By physical complaint box.
- Through an online internet or intranet platform.
- Verbally by telephone hotline or other voice messaging system.
- At a physical meeting within a reasonable time frame of the individual's request.

(Article 9(2) and Recital 53, Whistleblowing Directive.)

Organizations may also engage third parties to receive reports on their behalf, such as:

- External reporting platform providers.
- Outside counsel.
- Auditors.
- Trade union representatives.
- Employee representatives.

(Article 8(5) and Recital 54, Whistleblowing Directive.)

Reporting to EU and Member State Authorities

A whistleblower may report a concern to an EU or member state authority directly if:

- Internal reporting channels do not exist.
- Internal reporting channels do not function properly.
- An organization does not take appropriate action as part of an internal investigation.
- The reporter has valid reasons to believe that:
  - they will experience retaliation regarding an internal report;
  - the person involved in the wrongdoing is responsible for receiving internal reports;
  - there is a risk the organization will conceal or destroy evidence; or
  - the breach requires urgent action to safeguard health, safety, or the environment.

(Article 10 and Recitals 61 and 62, Whistleblowing Directive.)

Public Reporting

A whistleblower may contact the media or make a public disclosure to report a concern when:

- The whistleblower first reported internally or to an EU or member state authority and the reported violation was not appropriately investigated or remediated.
- There is a risk of retaliation and it is unlikely that an EU or member state authority will effectively address the violation due to the particular circumstances of the case, for example:
  - evidence may be concealed or destroyed; or
  - the authority may be involved in the reported violation.
- The whistleblower has reasonable grounds to believe there is an imminent or serious danger to the public interest or the risk of irreversible damage, including physical harm.

(Article 15 and Recitals 79 to 81, Whistleblowing Directive.)

Handling Internal Whistleblower Reports

Organizations should establish and document procedures for providing acknowledgment and feedback on whistleblower reports within the required time frame, maintaining the confidentiality and security of reports and investigations, and protecting all involved individuals' personal data.

Acknowledging and Clarifying Reports

The Whistleblowing Directive requires organizations to acknowledge receipt of a report to the whistleblower within seven days of receiving the report (Article 9(1)(b), Whistleblowing Directive). Organizations must then designate an impartial person to follow up on the report and communicate with the whistleblower, for example:

- A member of the organization's compliance, legal, or human resources groups.
- An external service provider engaged to help the organization administer the whistleblowing program.

(Article 9(1)(c) and Recitals 54 and 56, Whistleblowing Directive.)

Organizations may ask the whistleblower for further information during the investigation, but they cannot obligate or force the whistleblower to provide it (Article 9(1)(c) and Recital 57, Whistleblowing Directive).

Feedback and Time Frames

Organizations must diligently investigate each reported concern and provide verbal, written, or in-person feedback to the whistleblower within three months from either:

- The acknowledgment of receipt.
- The expiry of the seven-day period after the report was made if the organization did not acknowledge receipt of the report.

(Article 9(1)(f) and Recital 58, Whistleblowing Directive.)

If an organization has not determined its course of action within this time frame, it should inform the whistleblower of the delay and when to expect feedback (Recital 58, Whistleblowing Directive).

Feedback to whistleblowers must include:

- The action planned or taken following the report, for example:
  - referral to other channels or procedures if the report only affects the whistleblower;
  - referral to an EU or member state authority;
  - closure of the report based on lack of sufficient evidence or other grounds;
  - launch of an internal investigation; or
  - findings from an internal investigation and remedial measures.
- The grounds for the action planned or taken.

(Recital 57, Whistleblowing Directive.)

Organizations are not required to provide feedback to the whistleblower if doing so at the time would prejudice the investigation or affect implicated individuals' rights. However, in all circumstances, they must inform the whistleblower about the investigation's progress and outcome. (Recital 57, Whistleblowing Directive.)

Confidentiality, Security, and Data Protection

The Whistleblowing Directive requires organizations to:

- Operate their reporting channels in a secure manner and keep confidential the identities of:
  - the whistleblower;
  - any individuals assisting the whistleblower in making the report (facilitators); and
  - any third parties and implicated individuals contained in the report.

  (Articles 9 and 16, Whistleblowing Directive.)
- Process personal data regarding a whistleblower program according to the GDPR's requirements (Article 17 and Recital 83, Whistleblowing Directive; see Data Protection Law Requirements and Whistleblowing Hotlines).
- Maintain records of all reports received for only as long as necessary and proportionate to comply with the Whistleblowing Directive or other applicable laws (Article 18, Whistleblowing Directive).

Protections for Whistleblowers

The Whistleblowing Directive prohibits organizations from retaliating against whistleblowers for reporting concerns. Retaliation can take many forms, including:

- Suspension, layoff, dismissal, or equivalent measures.
- Demotion, transfer, wage reduction, or withholding of promotion or training.
- Change of work location or hours.
- A negative performance assessment or employment reference.
- Issuing any disciplinary measure, reprimand, or other penalty, including a financial penalty.
- Coercion, intimidation, discrimination, harassment, unfair treatment, or ostracism.

- Failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations of a permanent employment offer.
- Non-renewal or early termination of a temporary employment contract.
- Reputational harm, particularly on social media.
- Financial loss, including loss of business and loss of income.
- Blacklisting based on a sector or industry-wide informal or formal agreement.
- Early termination or cancellation of a goods or services contract.
- Cancellation of a license or permit.
- Psychiatric or medical referrals.

(Article 19 and Recitals 39 to 41, Whistleblowing Directive.)

The Whistleblowing Directive sets out measures to support whistleblowers and protect them against retaliation, including:

- **Advice.** Whistleblowers will have free access to comprehensive and independent information and advice on available procedures and remedies, protection against retaliation, and the whistleblowers' rights.
- **Remedial measures.** Whistleblowers will have access to appropriate remedial measures against retaliation, including:
  - interim relief to halt ongoing workplace retaliation, such as threats or harassment, or prevent termination pending the resolution of legal proceedings; and
  - a reversed burden of proof requiring organizations to prove that they are not retaliating against the whistleblower.
- **Protection from liability.** Whistleblowers will not be liable for breaching any contractual or legal restrictions on disclosing information (such as gag clauses) for making reports or disclosures through internal or external reporting channels.
- **Protection in judicial proceedings.** Whistleblowers may rely on the Whistleblowing Directive and its implementing laws for their defense in legal proceedings against them related to the report or disclosure.
- **Other measures.** Whistleblowers will have access to financial assistance and psychological support.

(Articles 20 and 21 and Recitals 87 to 99, Whistleblowing Directive.)

Protections for Implicated Individuals

The Whistleblowing Directive grants certain rights and protections to individuals implicated in a whistleblower's report, including:

- The presumption of innocence.
- The right to an effective remedy and a fair trial.
- The right to a defense, including the right to be heard.
- The right to access their file.
- Protection of their identity and personal data.

(Article 22 and Recital 100, Whistleblowing Directive.)

Penalties for Violations

The Whistleblowing Directive does not set out specific penalties for violations but instructs EU member states to incorporate effective, proportionate, and dissuasive penalties into their implementing laws. These penalties will apply to individuals or legal entities that:

- Hinder or attempt to hinder reporting.
- Retaliate against a whistleblower or related individuals or entities that could suffer retaliation.
- Bring vexatious proceedings against a whistleblower or related individuals or entities that could suffer retaliation.
- Breach the duty to keep the whistleblower's identity confidential.

(Article 23(1), Whistleblowing Directive.)

EU member state implementing laws must also include penalties for whistleblowers who knowingly report or publicly disclose false information and measures to compensate those damaged by a false report (Article 23(2) and Recital 102, Whistleblowing Directive).

Penalties of varying severity in EU member state implementing laws may create different levels of risk for organizations operating in more than one country.

Data Protection Law Requirements and Whistleblowing Hotlines

Organizations processing personal data in the context of a whistleblowing program must comply with the GDPR and its implementing laws (Article 17 and Recital 83, Whistleblowing Directive). Organizations subject to the GDPR must therefore check applicable EU member state laws for varying requirements (see GDPR National Implementation Legislation Toolkit and Practice Note, GDPR Data Protection Authority Guidance Tracker by Country (EEA)).

The Article 29 Working Party (now the European Data Protection Board (EDPB)) issued an Opinion on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime (WP117) (Feb. 1, 2006) (WP29 Opinion), which provides guidance on how to implement whistleblowing programs in compliance with the previous Data Protection Directive. Although the WP29 Opinion pre-dates the GDPR, many of the recommendations will likely remain relevant until the EDPB issues superseding guidance.

For a general overview of the GDPR's requirements, see Practice Notes, Overview of EU General Data Protection Regulation and General Data Protection Regulation (GDPR) Topic Index.

Legal Basis for Processing Personal Data

The GDPR requires organizations to have a legal basis for processing personal data, including personal data of whistleblowers, witnesses, and individuals implicated in whistleblowing reports (Article 6, GDPR). For processing personal data relating to whistleblowing reports, EU organizations typically rely on the grounds that the processing is necessary to:

- Comply with the organization's legal obligations (Article 6(1)(c), GDPR). Once the Whistleblowing Directive takes effect, organizations will likely point to the legal obligations it imposes to establish an internal reporting system and related controls.
- Pursue the organization's legitimate interests (Article 6(1)(f), GDPR).

When an organization relies on its legitimate interests as a legal basis for processing, it should prepare a Legitimate Interest Assessment (LIA) that documents the organization's interests in receiving and investigating whistleblowing reports and the reasons that these interests prevail over the interests of whistleblowers and other concerned individuals.

For more information on the legal bases for processing personal data under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation: Lawfulness of processing.

Special Categories of Personal Data

The GDPR imposes additional restrictions on organizations processing special categories of personal data, which may include personal data revealing:

- Racial or ethnic origin.
- Political opinions.
- Religious and philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data for uniquely identifying a natural person.
- Data concerning health.
- Sex life and sexual orientation.

(Article 9(1), GDPR.)

Organizations collecting special categories of personal data through whistleblower programs must meet one of the exceptions to the GDPR's general prohibition on processing this data in addition to establishing a legal basis for the processing under GDPR Article 6 (Article 9(2), GDPR). For more information on processing special categories of data, see Practice Note, Overview of EU General Data Protection Regulation: Special categories of personal data.

Data Protection Impact Assessment

Organizations must conduct a data protection impact assessment (DPIA) before undertaking any processing that presents a specific privacy risk by virtue of its nature, scope, or purposes (Article 35, GDPR). A DPIA is a formal procedure through which organizations can evaluate the impact of data processing activities on personal data protection.

EU member states have also published their own lists detailing when DPIAs are required and when they are not. Operating a whistleblowing program will likely trigger a need for a DPIA in several EU member states. Multinational organizations may conduct one DPIA for their pan-EU or global whistleblowing program instead of separate DPIAs for each EU member state that requires one.

For more information on DPIAs, see Practice Note, Overview of EU General Data Protection Regulation: Data protection impact assessment. For more information on EU member state DPIA lists, see Practice Note, GDPR Data Protection Authority Guidance Tracker by Country (EEA).

Notice

The GDPR requires organizations to provide data subjects with a privacy notice before or when they collect personal data (Articles 13 and 14, GDPR). Organizations should address personal data collection for whistleblower programs in a specific whistleblowing privacy notice that includes the information set out in GDPR Articles 13 and 14 along with information about the organizations' whistleblowing programs and procedures.

Organizations should make the whistleblowing privacy notice available to all potential whistleblowers on all channels before collecting any personal data through the whistleblowing program, including:

- On the whistleblowing program's online platform where whistleblowers can report their concerns.
- Through the whistleblowing program's telephone hotline using:
  - a layered telephone script that covers the main topics of the whistleblowing privacy notice; and
  - the hotline's technical capabilities to provide callers with additional detail in an easily accessible and understandable manner.
- Other channels, for example, providing a hard copy of the whistleblowing privacy notice before the whistleblower shares their concerns at an in-person meeting.

Organizations also must provide the privacy notice to individuals implicated in the report before beginning the investigation. However, organizations may postpone notifying implicated individuals if doing so would prejudice the investigation or result in destruction of potential evidence.

For more information on the GDPR's privacy notice requirements, see Practice Note, Data Subject Rights Under the GDPR: Information Right. For a sample whistleblower privacy notice, see Standard Document, Whistleblower Hotline Privacy Notice (Non-US).

Data Security

The GDPR requires organizations to implement appropriate technical and organizational measures to ensure a level of security appropriate to the specific personal data and processing activities. Organizations with whistleblowing programs must account for the risks presented by accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data they collect and process. (Article 32, GDPR.) For more information on the GDPR's data security requirements, see Practice Note, Overview of EU General Data Protection Regulation: Data security. For more information on developing an information security program, see Global Information Security Toolkit.

Third-Party Service Providers

Organizations frequently engage third parties to perform functions on their behalf, including operating their whistleblower reporting channels. The GDPR requires organizations to enter into contracts with third-party whistleblowing service providers (processors) that contain specific obligations (Article 28(3), GDPR). Organizations should periodically verify the processor's compliance with these obligations. Organizations should also conduct privacy and security due diligence on these service providers before engaging them (Article 28(1), GDPR).

For more information on processor obligations under the GDPR, see Practice Note, Data Processor Obligations Under the GDPR. For more information on conducting third-party due diligence, see Managing Vendor and Service Provider Cyber Risks Toolkit.

Data Breach Notification

The GDPR requires organizations that experience a data breach that results in a high risk to data subjects' rights and freedoms to notify:

- The appropriate EU member state supervisory authority no later than 72 hours after learning of the breach.
- The affected data subjects without undue delay.

(Articles 33 and 34, GDPR.)

If a breach affects personal data related to a whistleblowing report and results in a high risk to those data subjects, organizations must notify the supervisory authority and affected data subjects accordingly, including the whistleblower and implicated individuals.

For more information on the content of data breach notifications and exceptions to these requirements, see Practice Note, Overview of EU General Data Protection Regulation: Data security breach. For more information on data breach response, see Global Cyber Incident Response and Data Breach Notification Toolkit.

Data Retention

Neither the GDPR nor the Whistleblowing Directive set out specific retention periods for personal data (Article 18, Whistleblowing Directive; see Confidentiality, Security, and Data Protection). The GDPR requires organizations to retain personal data only for the time necessary to fulfill each specific processing purpose, unless otherwise required by applicable EU or member state law (Article 25(2), GDPR). The WP 29 Guidance notes that organizations should:

- Delete personal data processed in the context of a whistleblowing hotline promptly, usually within two months of completing the investigation into the facts alleged in the report.
- Retain personal data related to legal proceedings or disciplinary measures initiated against the incriminated person or the whistleblower in cases of false or slanderous reports until the conclusion of these proceedings and the relevant appeal period, which is determined by EU member state law.
- Delete personal data relating to unsubstantiated whistleblowing reports without delay.

These requirements may change in the future based on:

- EU member state laws implementing the Whistleblowing Directive.
- EU member state regulatory guidance.
- EDPB guidance.

EU member state labor and employment laws often require specific retention periods for employee data and records related to whistleblowing allegations. The details of these laws are outside the scope of this Note.

Cross-Border Data Transfers

GDPR Chapter V imposes several obligations on organizations that transfer personal data outside the EU to third countries not deemed by the European Commission as providing an adequate level of data protection. Transfers under the GDPR also occur when personal data kept on EU servers is remotely accessed from outside the EU, for example, by a service provider.

Organizations with whistleblowing programs should ensure they:

- Identify and document their mechanisms for transferring personal data related to whistleblowing reports outside the EU in compliance with the GDPR, including the latest developments related to the ECJ's decision in Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Case C-311/18) EU:C:2020:559 (*Schrems II*).
- Include information on the relevant transfers and mechanisms in their privacy notice (see Data Protection Impact Assessment).

For more information on transferring personal data outside the EU, see:

- Practice Note, Overview of EU General Data Protection Regulation: Cross-border data transfers.
- GDPR Cross-Border Transfers Checklist.
- GDPR Data Protection Authority Guidance Tracker by Country (EEA).
- Article, European Commission's International Data Transfer Standard Contractual Clauses: What Businesses Need to Know.
- Article, EDPB Supplementary Measures Recommendations and German DPA Guidance Post Schrems II.
- Legal Update, Schrems II: controller to processor standard contractual clauses valid but EU-US Privacy Shield invalid (ECJ).

Data Subject Rights

GDPR Chapter III provides data subjects with certain rights related to their personal data, including access, correction, erasure, processing restriction, and data portability. These data subject requests are often problematic in the whistleblower context, for example, if an individual who is the subject of an investigation requests access to information on the whistleblower or the status of the investigation for interfering with its progress.

Organizations should put into place a standard operating procedure with well-trained personnel to handle data subject requests while:

- Keeping the identities of the whistleblower, witnesses, and implicated individuals confidential.
- Protecting the integrity of the investigative process.
- Complying with the GDPR and member state implementing laws.

For more on data subject rights under the GDPR, see Practice Note, Data Subject Rights Under the GDPR.

Records of Processing Operations

GDPR Article 30 requires organizations to maintain detailed documentation about the data processing activities under their responsibility, which includes operating a whistleblowing program. Organizations should prepare an Article 30 record that covers their whistleblowing processing operations specifically.

For more on documenting processing activities under the GDPR, see Practice Note, Demonstrating Compliance with the GDPR: Record of Processing Activities and Standard Document, Record of Processing Activities Under Article 30 (GDPR).

Implementing a Whistleblower Program

Since the EU Whistleblowing Directive only sets minimum standards for each of the 27 EU member states to implement into their national laws, the laws on whistleblowing programs will not be fully harmonized across the EU. Multinational organizations with operations in several EU member states might therefore need to comply with potentially differing requirements in each location.

While the EU member states work to adopt implementing laws before the December 17, 2021 deadline, organizations should prepare their

whistleblowing programs for compliance with the Whistleblowing Directive while monitoring the implementing laws' progress and supervisory authority guidance. Organizations with already existing whistleblowing hotlines or programs will need to update their processes and procedures to comply with the new rules, and organizations without them will need to build a program from the ground up.

When establishing or updating a whistleblowing program to comply with the Whistleblowing Directive, organizations should:

- Determine whether to build the whistleblowing program internally or with a third-party service provider. Most organizations rely on an external service provider for their expertise and to save internal resources. If retaining a third-party service provider, organizations should:
  - conduct privacy and security due diligence on the selected vendor before finalizing the engagement; and
  - enter into a service contract with the vendor that includes data processing clauses that comply with GDPR Article 28 and, if applicable, data transfer clauses that comply with the GDPR's requirements on transfers to third countries.
- Understand the scope of reportable concerns, as applicable EU member state implementing laws may permit reports about violations beyond those in the Whistleblowing Directive.
- Determine which works council and union procedures will apply in each country (for example, prior consultation or approval) and ensure they can comply.
- Determine whether to set up separate reporting channels in each country or use an EU-wide or global reporting mechanism, considering:
  - EU member state implementing law requirements and supervisory authority guidance on the permissibility of local versus centralized reporting channels, when released;
  - the organization's risk appetite;
  - which arrangement would best encourage whistleblowers to report concerns internally instead of externally;
  - which arrangement would provide the most consistency, efficiency, impartiality, and confidentiality when an organization has many different locations; and
  - whether the requirements of applicable EU member state implementing laws are similar or vastly different.
- Decide what types of channels to set up for whistleblowers to report their concerns, including a process for scheduling in-person meetings to receive reports within a reasonable time frame of a whistleblower's request.
- Make new and existing whistleblower reporting channels available externally to individuals like former employees, job applicants, trainees, potential vendors, suppliers, subcontractors, volunteers, and business partners.
- Draft and provide privacy notices for whistleblowers and implicated individuals with sufficient information about the internal and external reporting processes and the investigation and feedback process.
- Draft internal policies and procedures that set out the whistleblowing program's structure and operation to ensure uniform application of whistleblowing and investigation requirements across the corporate group.
- Design the reporting, investigation, and feedback processes to be user friendly, easily accessible, and transparent, including, for example:
  - reporting channels that are available 24 hours per day, 7 days per week;
  - offering anonymity if EU member state law permits;
  - using local languages; and
  - providing transparent explanatory information and simple instructions.
- Designate a person or department responsible for investigating whistleblowing reports in an independent and impartial manner, entirely free of any conflict of interest.
- Set up or update their internal investigations protocols to ensure that designated and well-trained individuals investigate each report in a consistent manner in compliance with legal and regulatory requirements, regardless of the whistleblower's location, the implicated individuals, or the reported violations.
- Preserve the anonymity of anonymous whistleblowers when applicable EU member state law permits anonymous reporting. Organizations should establish a mechanism that permits them to contact anonymous whistleblowers for clarifications without knowing the whistleblowers' identity, for example, through a specific coding system.
- When requesting clarifying information from a whistleblower, not pressure them to provide additional information when requesting clarifications about the reported concern. Train investigators to instead:
  - ask for additional information in a manner that elicits the most helpful response; and

  - stop the questioning if the whistleblower indicates directly or through silence that they do not want to provide any further information.
- When providing feedback to whistleblowers, consider providing more frequent updates, such as every two weeks, instead of waiting for the three-month deadline to approach. If a whistleblower does not hear from the organization for one or two months, they might conclude that the organization is not taking their report seriously and revert to an external reporting channel.
- Make clear that the organization has zero tolerance for any kind of retaliation and will discipline or terminate anyone who retaliates against a whistleblower. Organizations should include this in their code of conduct and other relevant policies, and regularly train their employees on the prohibition against retaliation.
- Set up an independent process for whistleblowers to make a complaint that the organization is not taking their original report seriously, is retaliating against them, is pressuring them to provide more information, or if they are otherwise concerned about the process.
- Publicize the whistleblowing program within the organization and conduct training for employees and other workers.
- Review the whistleblowing program's operations periodically and address any challenges promptly.
- Comply with the GDPR and applicable EU member state data protection laws when collecting or processing personal data through their whistleblowing program, including:
  - processing personal data lawfully and with an appropriate legal basis;
  - conducting a LIA when relying on the organization's legitimate interest for the processing;
  - using personal data for a new purpose only when compatible with the original collection purpose;
  - adhering to the rules for processing special categories of personal data and criminal conviction and offense data;
  - providing a detailed and easy to understand privacy notice to individuals about processing their personal data through the whistleblowing program;
  - responding to data subject rights requests;
  - implementing appropriate data retention time frames;
  - engaging service providers that implement appropriate safeguards to meet the GDPR's requirements;
  - entering into contracts with service providers that contain appropriate data protection language and regularly monitoring the service provider's compliance with the contract;
  - keeping appropriate Article 30 records of their processing activities;
  - implementing measures to adequately secure personal data according to its sensitivity;
  - handling security breaches according to the GDPR's requirements, including notifying the supervisory authority and affected data subjects if required;
  - conducting a DPIA when required; and
  - transferring personal data to third countries in compliance with the GDPR's rules and supervisory authority guidance following *Schrems II*.