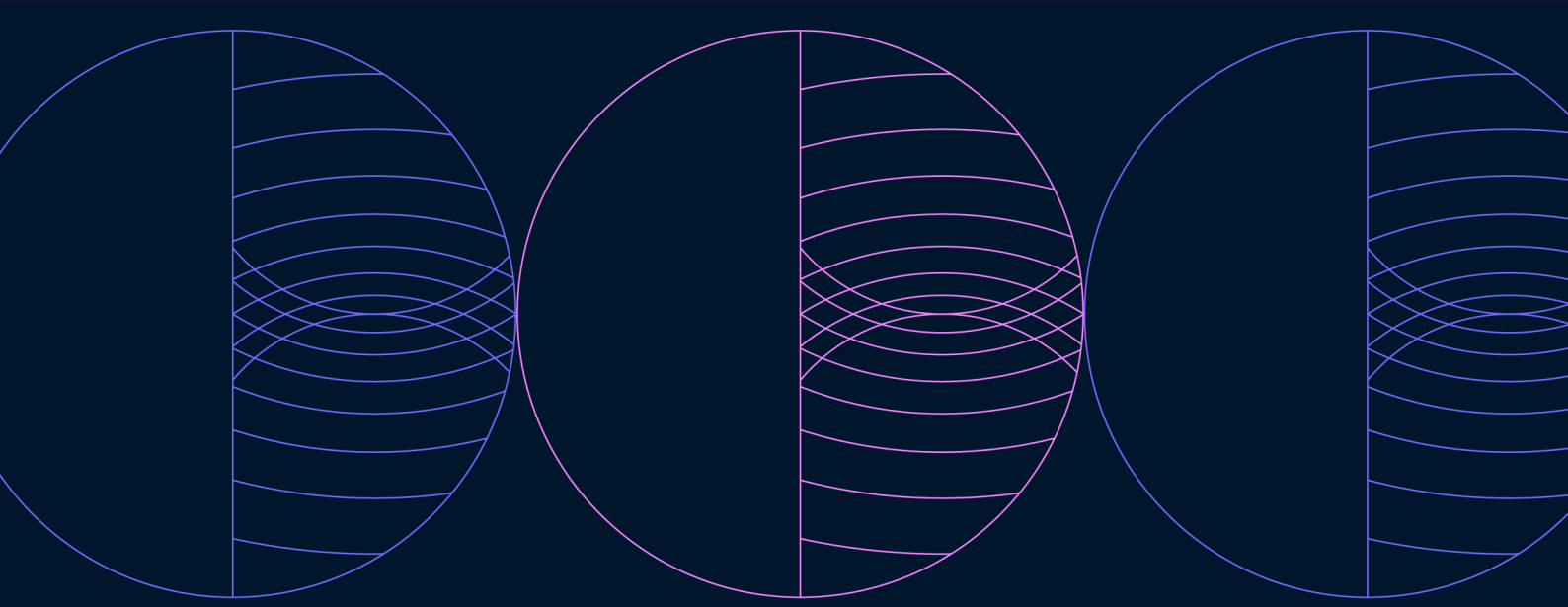
IN-HOUSE VIEW

# Whistleblowing

## EU AND UK DATA PROTECTION IMPLICATIONS OF WHISTLEBLOWING PROCEDURES



LEXOLOGY

# Whistleblowing

2024

Contributing Editors

**Silvio Cavallo and Marco Lucci**

Pillarstone

**Generated: August 1, 2024**

# EU and UK Data Protection Implications of Whistleblowing Procedures

**William Mallin**, **Vishnu Shankar**, **Chris Warren-Smith** and **Matthew Howse**
Morgan, Lewis & Bockius LLP

## Summary

## Introduction

This chapter considers the key data protection issues arising at the intersection between EU and UK (collectively known as Europe) data protection laws and whistleblowing procedures. Whistleblowing, data privacy and cybersecurity (collectively known as data protection) considerations and obligations often overlap, potentially conflict and create novel issues for legal and compliance teams. The aim of whistleblowing procedures is to provide safe channels for individuals to report fraud, corruption and other serious wrongdoing or irregularities in organisations. Notably, many relevant employment laws are primarily concerned with the rights of the whistleblower whereas data protection legislation has a broader focus on identified or identifiable persons involved in the overall process. Further, global whistleblowing frameworks continue to be developed or proposed that require, amongst other things, certain organisations to develop anonymous whistleblowing hotlines or whistleblower protection programmes, including in compliance with data protection legislation.

There are multiple laws in EU member states and the UK which apply to whistleblowing, including the EU Whistleblowing Directive (2019/1937), which is required to be transposed into EU member state law. Similarly, the EU General Data Protection Regulation, the UK General Data Protection Regulation and companion data protection laws (collectively, the GDPR) apply to the processing of personal data in relation to the organisations' activities in the European Economic Area and the UK. Whistleblowing will almost inevitably involve the processing of personal data, including that of the whistleblower, witnesses, alleged wrongdoers and potentially other persons (including employees, contractors, suppliers and business partners). Therefore, the GDPR's rights and obligations may apply in relation to an organisation's whistleblowing procedures (including helplines, whistleblower protection measures and data security arrangements) even for those organisations established outside of Europe because of the GDPR's extra-territorial application.

Given the nature of whistleblowing disclosures, 'special category' personal data, criminal offence data or other forms of sensitive personal data may often be involved, which may trigger enhanced responsibilities under the GDPR. However, the specific GDPR requirements to consider in each case will depend on the nature of the whistleblowing disclosure, the ensuing investigation and whether the controller operates its own whistleblowing procedures or outsources these to a third-party provider (including potential transfers of personal data outside Europe).

## Balancing confidentiality with other key objectives

For whistleblowing procedures to be effective, individuals may need to know that their identity will be appropriately protected if they report concerns. The confidentiality of the process is also important to those accused of wrongdoing and to other witnesses involved. That said, organisations may wish to be thoughtful about committing to keep the identity of the whistleblowers or accused confidential in every circumstance; notably, fairness and due process considerations may, in certain circumstances, require the disclosure of the identity of the whistleblower and other persons involved. In fact, there may even be GDPR considerations (such as in connection with the GDPR's transparency obligations

considered further below) which may warrant such disclosures. Notably, certain European supervisory authorities (SAs) suggest that employers do not encourage reporting on an anonymous basis. Therefore, organisations may, based on the relevant circumstances, either require that employees submit anonymous reports, or identify themselves and agree to their identity being potentially disclosed. Further, there may be potentially different and even conflicting approaches to whistleblowing outside of Europe; for example, organisations subject to the US Sarbanes-Oxley Act 2002 must usually provide an anonymous procedure for reporting concerns about auditing or accounting irregularities.

Overall, multinational organisations seeking to adopt a consistent whistleblowing process across their corporate group on a global basis (and even within Europe) may encounter certain material challenges, including because of data protection laws such as the GDPR and positions adopted by certain SAs. Nonetheless, whatever the jurisdiction, maintaining the confidentiality of the whistleblowing file is a key objective. As a result, organisations will need to, for example, implement appropriate procedures to ensure that access to the file occurs on a need-to-know basis only and that staff with access are subject to appropriate obligations of secrecy.

## Data protection and whistleblowing

### Categories of personal data implicated in whistleblowing

Information that is considered personal data will almost always be implicated in a whistleblowing context. Further, sensitive categories of data, such as special category personal data and criminal convictions and offences data may also be processed in relation to whistleblowing procedures, the processing of which is subject to enhanced restrictions under the GDPR.

- Special category data refers to data revealing the following: racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership; the processing of genetic data; biometric data for uniquely identifying a person; data concerning health; or data concerning a person's sex life or sexual orientation. Whistleblowing may implicate such categories of data if (for example) the whistleblower alleges workplace discrimination with respect to such demographic characteristics. Under the GDPR, processing these types of data is restricted unless the controller can demonstrate that a GDPR 'lawful basis' and one GDPR-specific 'condition' apply to such processing. In a whistleblowing context, commonly relied upon conditions include the employment, social security and social protection law condition under article 9(2)(b) GDPR and the defence of legal claims condition under article 9(2)(g) GDPR.
- Personal data relating to criminal convictions and offences, or related security measures, is not special category data but is nonetheless subject to enhanced protection under the GDPR. Importantly in a whistleblowing context, criminal offence data is not just about specific criminal convictions or trials but also potentially extends to personal data relating to unproven allegations and information relating to the absence of convictions. The GDPR requires that the processing of such data needs to be authorised by domestic EU member state or UK law, as applicable. In the UK, for example, the controller would need to satisfy the conditions set out in Schedule

1 of the Data Protection Act 2018 (unless the controller is a public body or a private body carrying out a public sector task), such as conditions applicable to preventing or detecting unlawful acts and preventing fraud (which may be applicable to certain whistleblowing cases).

There are additional requirements applicable to the processing of special category data and criminal convictions and offences data. For example, in the UK, reliance on the employment, social security or social protection (and the unlawful acts and fraud conditions) in the context of both special category data and criminal conviction data requires the controller to put in place, review and update (as necessary) an 'appropriate policy document'. This document, which may need to be produced to the UK's SA (the Information Commissioner's Office) would explain the organisation's procedures for complying with data protection principles when processing this data and describe its procedure in respect of data retention and erasure.

## Transparency obligations

Controllers must provide data subjects with certain information prescribed by the GDPR with respect to how the controller will process personal data relating to such data subject. In a whistleblowing context, most organisations will usually attempt to satisfy this requirement by relying on their pre-existing and general employee data protection notice (DP Notice), which explains how employees' personal data is used by their employer, including in relation to whistleblowing procedures. In some cases, however, it might be necessary to develop and deploy a more bespoke DP Notice should the specific circumstances of the case dictate this or if the general DP Notice is too broad to provide sufficient information about how personal data will be processed in connection with the whistleblowing process specifically. For example, certain controllers provide a DP Notice specifically with respect to whistleblowing hotlines which is made available online or discussed verbally on the hotline itself.

There are additional GDPR and transparency complexities in a whistleblowing context. The GDPR requires that individuals are provided with a DP Notice if their data has been obtained from a third party (i.e., other than from the data subject themselves). Such DP Notices would need to identify the source from which the personal data originated. This obligation may potentially conflict with confidentiality obligations to, or expectations of, the whistleblower or witnesses.

DP Notices are typically required to be provided by the controller within a month of receiving the data. However, there are exemptions to this obligation if complying with the obligation to provide the information would seriously impair the achievement of the objectives of that processing. Specifically, it is arguable that because disclosing the identity of the source of the personal data in a whistleblowing context (i.e., the whistleblower) could undermine the whistleblowing process, providing a DP Notice to the relevant individuals is not necessary. However, with respect to anonymous whistleblowing reports, the obligation under article 14(2)(f) GDPR could arguably require only disclosing that the report came from a whistleblower, but not which whistleblower specifically.

## GDPR lawful basis

A fundamental principle under the GDPR is that controllers must identify a legal basis for processing personal data. This includes personal data of whistleblowers, witnesses and other individuals implicated in the process or otherwise identifiable. The commonly relied upon lawful bases are that the processing is necessary for:

- compliance with a legal obligation to which the controller is subject (article 6(1)(c) GDPR); or
- the purposes of the legitimate interests pursued by the controller (article 6(1)(f) GDPR), including the prevention of misconduct, corruption or wrongdoing. The controller in these circumstances will need to demonstrate why its interests in furthering the whistleblowing procedure outweigh the interests of the whistleblower and other data subjects involved.

While relying on consent under article 6(1)(a) GDPR as the lawful base is possible in theory, this may cause issues in practice. The potential imbalance of power between the employer or other investigating body on the one hand, and the employee or other individual making the disclosure,on the other hand, may discredit the freely given nature of consent, as required under the GDPR. Further, consent, even if granted, may be withdrawn at any time. This may, in turn, impact the overall whistleblowing process.

## Data protection impact assessments and GDPR SA approvals

Where processing presents a specific privacy risk by virtue of its nature, scope or purposes, controllers must conduct a data protection impact assessment (DPIA). Certain EU member state SAs presumptively treat personal data processing in relation to whistleblowing helplines as requiring DPIAs (such as the French SA). DPIAs may be a potentially time-consuming exercise and may be a 'gating item' with respect to certain whistleblowing procedures. However, it may be possible for multinational organisations to conduct one DPIA for their pan-EU or global whistleblowing programme instead of separate DPIAs for each EU member state that requires one.

Although the UK's Information Commissioner's Office does not need to approve a whistleblowing hotline, in many other European countries, it may be necessary to obtain approval from other EU member state SAs before collecting and processing personal data under a whistleblowing scheme, and in certain EU member states (such as Sweden and Hungary) potentially restrictive conditions need to be satisfied before the SA will approve such schemes.

## Rights of data subjects under the GDPR, including the right of access

The GDPR affords data subjects with certain rights. In addition to the right to information described above, rights of access, rectification, erasure, restriction, data portability and objection apply in certain circumstances. Given the sensitivities involved, controllers operating whistleblowing schemes may be subjected to particularly challenging circumstances, particularly in relation to the right of the data subject to obtain access to and copies of their data (known as the data subject access right).

Data subject access requests are common in a whistleblowing context. Dealing with access requests is particularly complex in these circumstances given the conflicting obligations

and duties of care that an organisation owes to the individuals involved in the process. The amount and sensitivity of the data held will depend on whether the request is made by the accused, the whistleblower, a witness or some other third party. A controller's response to an access request must involve a balancing exercise of the requester's right of access against the whistleblower and other individuals' rights. There are also certain limited exemptions from the right of access that can permit a data controller to withhold some or all the personal data involved.

Notably, controllers may wish to consider the exemption relating to the protection of the 'rights of others'. For example, the UK's Data Protection Act 2018 states that controllers do not have to comply with an access request if doing so means disclosing information which identifies someone else, except where that other person consents to the disclosure or it is reasonable to comply with the request without that person's consent. To determine whether it is reasonable to comply without consent, controllers are required to consider all the relevant circumstances, including the type of information that would be disclosed, any duty of confidentiality it owes to the other people, any steps it took to try to get the other person's consent, whether the other person is capable of giving consent and any stated refusal of consent by the other person. If applicable, this exemption may allow the controller to withhold a whistleblowing report (all or part of it) on the basis that it contains the personal data of, for example, the whistleblower, and they did not consent to disclose this information to the requester and it would not be reasonable given the information concerned to disclose it without their consent.

Controllers may also wish to consider the crime and taxation exemption under the GDPR. It could be possible that disclosing a whistleblowing report would prejudice the ongoing investigation into alleged fraud or corruption, disclose the identity of the whistleblower and potentially subject them to negative treatment. On this basis, it might be permissible to rely on the crime and taxation exemption (as well as choosing not to disclose the report on the basis that it identifies other individuals). The UK SA explicitly mentions this exemption in its guidance concerning data subject access requests.

It may also be possible to refuse to comply with an access request entirely if the request is manifestly unfounded or manifestly excessive, although this exemption is narrowly construed.

## Data retention and data minimisation

As a general principle, data controllers must not process personal data for longer than is necessary for the purposes for which the personal data is processed. Many organisations design data retention policies and schedules so that they can effectively govern how different types of data are retained and disposed of responsibly and securely. There are no prescribed data retention periods under the GDPR for types of personal data, although often other non-privacy related legislation sets out minimum or maximum periods of retention for specific types of data.

Many organisations consider implementing different retention schedules depending on whether the whistleblowing disclosure leads to an investigation or not. Conversely, many organisations elect to delete personal data relating to whistleblowing disclosures that are not investigated within a few months following the initial whistleblowing report. For example, in the UK, employers generally retain employment-related personal data for seven years

to allow for the six-year limitation period for most English civil law claims in addition to an extra year to account for the time it could take for a claim to commence.

Another key GDPR principle is that the personal data that controllers process is adequate (i.e., sufficient to fulfil the relevant purpose), relevant (i.e., there is a rational link between the data collected and the purpose) and limited to what is necessary (i.e., excess personal data is not processed relative to the intended purpose). Controllers may wish to document a whistleblowing investigation's scope and undertake a personal data proportionality assessment, to demonstrate that data minimisation principles have been applied.

## Data security and breach notification

As is generally the case, data controllers must implement appropriate technical and organisational security measures to keep personal data secure, including, if appropriate, encryption, pseudo-anonymisation, back-ups, and systems resilience mechanisms, and they must test the effectiveness of these measures. The measures implemented will need to reflect the sensitive nature of personal data that will likely be processed in a whistleblowing context. Common appropriate measures adopted in these circumstances include encryption, access controls and strong passwords.

By way of illustration, the Italian SA fined Bologna airport €40,000 in 2021 for allegedly violating the GDPR in respect of its whistleblowing systems. In particular, the airport had (allegedly) not used any encryption mechanisms for the transmission and storage of personal data. The lack of consideration to the privacy by design principle and a DPIA were also relevant in the SA'sassessment (these obligations are considered elsewhere in this chapter).

Given the types of personal data processed in connection with a whistleblowing investigation, a personal data breach affecting personal data relevant to a whistleblowing procedure may potentially result in a 'risk' or even 'high risk' to the affected data subjects. The appropriate GDPR SA would need to be notified 'without undue delay' and 'where feasible' within 72 hours after the controller becomes aware of the breach. The affected data subjects would need to be notified by the controller without 'undue delay' (should the breach present a high risk to the affected data subjects).

## Outsourcing of whistleblowing procedures

Many organisations elect to outsource certain aspects of their whistleblowing programme to a third-party service provider (such as the operation of an ethics hotline service). In all cases where a controller engages another entity to process personal data on their behalf, the controller must only use processors that provide sufficient guarantees to implement appropriate technical and organisational measures to ensure that data subject rights are protected. In this respect, due diligence may be appropriate into any third party engaged to provide whistleblowing services so that the organisation has discharged this obligation. Further, there are specific requirements under the GDPR in terms of the content of the contract that must be put in place between the controller and the processor, including where a third party has been engaged to operate an ethics hotline.

## International data transfers

If a third-party processor is based in a different country to the organisation or if the organisation is a multinational organisation that transfers personal data internally, the organisation will need to consider its GDPR obligations in connection with the international transfer of personal data. This will include, where necessary, documenting and implementing the legal transfer mechanism relied upon as its appropriate safeguard for the transfer, and making sure this is appropriately explained in the relevant DP Notice. Depending on the jurisdictions involved, the transfer may require the completion of a transfer risk assessment in addition to implementing the applicable appropriate GDPR safeguard (such as EU-approved standard contractual clauses). Conversely, any transfers between EU member states or between the UK and EU member states will not require any additional safeguards in the usual way, as well as any transfers from the UK or the EU to other third countries deemed adequate by the UK or the European Commission (e.g., Switzerland, New Zealand and South Korea).

The GDPR does contain (narrowly construed) exceptions or derogations from the requirement to put in place an appropriate safeguard for restricted transfers. For example, a transfer to a third country not benefitting from an adequacy decision can take place if the transfer is necessary for important reasons of public interest. Public interest in this context requires that the particular public interest is recognised in EU, EU member state or UK law. The public interest that whistleblowing frameworks are designed to achieve is arguably recognised in the EU Whistleblower Directive. That said, derogations from the applicable international data transfer obligations are, in general, narrowly construed and using a GDPR safeguard may be preferable where available.

## Privacy by design; documentation and accountability; data protection officers

A key GDPR principle is the requirement to integrate data protection into processing practices from the outset and throughout the life cycle of the activity. In a whistleblowing context, for example, when setting up an ethics hotline, an organisation should consider some privacy by design strategies such as encryption, pseudonymisation, data minimisation and functionality for data deletion.

Under the GDPR, controllers must demonstrate compliance with GDPR principles. This includes, where appropriate, the appointment of a data protection officer (DPO). As such, organisations may need to consider drafting and maintaining appropriate GDPR-related documentation that explains how it complies with its data protection obligations in connection with its whistleblowing framework. Appropriate documentation in this context will likely include a record of processing activities, data protection policies, data retention policies, legitimate interest assessments and breach logs.

Controllers are required to appoint a DPO in certain circumstances under the GDPR. Nonetheless, the operation of a whistleblowing procedure on its own does not require the appointment of a DPO. That said, if an organisation's whistleblowing activities mean that it engages in large-scale data processing or any of the other requirements for the appointment of a DPO are met, then such an organisation may need to appoint a DPO. Of course, the relevant organisation may have already appointed a DPO owing to its other data processing activities.

Where a DPO has been appointed, they may need to be involved in the planning and implementation of an organisation's whistleblowing model at an early stage. For example, the DPO may need to consider whether a DPIA is necessary in connection with the introduction of the relevant model and, if so, carry it out in a documented manner. Some organisations designate the DPO as the individual to whom whistleblowing reports must be made. In this regard, issues relating to personal data that might arise from the process can be given due consideration from the outset. Under the GDPR, the DPO is bound by secrecy or confidentiality concerning the performance of their tasks. On this basis, the DPO's involvement in the process may help the proper resolution of a whistleblowing investigation given the importance of confidentiality throughout the procedure.

## Conclusion

Many whistleblowing procedures involve potentially significant challenges; for instance, whistleblowers may be victimised, and an alleged wrongdoer's reputation may be damaged if the allegations turn out to be baseless or otherwise unfounded. While GDPR compliance may potentially add additional layers of complexity, it may also help to address certain of these more general challenges. Notably, an organisation with a robust GDPR compliance process (such as with respect to the appropriate handling of whistleblowing-related data) may be in a better position to create a trusted platform for employees and other individuals to raise legitimate concerns.

Morgan Lewis

| | |
|---|---|
| **William Mallin** | william.mallin@morganlewis.com |
| **Vishnu Shankar** | vishnu.shankar@morganlewis.com |
| **Chris Warren-Smith** | chris.warren-smith@morganlewis.com |
| **Matthew Howse** | matthew.howse@morganlewis.com |

Morgan, Lewis & Bockius LLP