Implementing a global corporate whistleblowing policy: data protection issues

Produced in partnership with **Pulina Whitaker and Lee Harding of Morgan, Lewis & Bockius LLP**

Companies must find a reliable method of identifying and correcting any unlawful or unethical conduct that occurs within their organisations in order to achieve effective corporate governance. In part, this objective can be achieved through the establishment of internal whistleblowing schemes, providing employees with a trusted and confidential mechanism for reporting misconduct.

Globally, there is an increasing trend for national legislation to require companies to establish internal financial control procedures—these are often implemented by way of whistleblowing schemes. The US still leads the way in providing strong standards for internal reporting and investigation of potential wrongdoing under the **Sarbanes-Oxley Act 2002** (SOX). For a US-regulated multi-national company, it can be difficult to create a consistent corporate whistleblowing scheme in all of the countries in which it operates. Further, in Europe, there is a need for organisations to balance their corporate governance objectives against the need to safeguard the privacy rights of those persons identified as a result of the operation of their whistleblowing scheme, particularly where reports under the scheme are made on an anonymous basis.

The introduction of **Regulation (EU) 2016/679**, the General Data Protection Regulation (GDPR) in the EU, has made privacy rights even more stringent, increasing the need to carry out whistleblowing procedures with careful internal checks and controls.

References:

Sarbanes-Oxley Act 2002

Corporate whistleblowing requirements

A company that operates in several jurisdictions worldwide and wishes to implement one, global whistleblowing policy, will need to take account of the legislative and regulatory requirements applicable in all those jurisdictions. Outlined below are the whistleblowing requirements in:

- the UK
- the US, and
- other EU jurisdictions

UK statutory requirements

In the UK, all employees and workers are protected against retaliatory action from their employer (such as dismissal or demotion) in response to protected whistleblowing disclosures under the **Public Interest Disclosure Act 1998** (**PIDA 1998**), which is now incorporated into the **Employment Rights Act 1996** (**ERA 1996**). This protection applies irrespective of whether a company is required to have an internal whistleblowing scheme. See **Whistleblowing—overview**.

There is no qualifying period of employment required to bring a whistleblowing claim. Employees and those falling into a wider definition of 'worker' (including certain agency workers, persons not working at the employer's premises, medics, dentists, judicial officer-holders and those undertaking certain work experience) are entitled to protection. For further information, see Practice Note: **Entitlement to claim whistleblowing**.

References:

Public Interest Disclosure Act 1998

In broad terms, to fall within scope of the protection, an employee or worker must make a disclosure of information which, in the reasonable belief of the employee making the disclosure, is made in the public interest and tends to show that a person (usually the employer) has failed, is failing or is likely to fail to comply with any legal obligation to which they are a subject. The alleged wrongdoings covered by the UK whistleblowing legislation is far broader than SOX in that it, for example, covers criminal offences, breaches of legal obligations, danger to health and safety and damage to the environment.

For a report to be a 'qualifying disclosure' under **ERA 1996**:

References:

ERA 1996, s 43B

- it must be a disclosure of relevant information, ie more than a threat, allegations without evidence or gathering of evidence
- information about a relevant failure: criminal offence, breach of legal obligation, miscarriage of justice, health and safety affecting an individual, damage to the environment, or the deliberate concealment of any of the preceding failures
- the employee or other worker has a reasonable belief that the disclosure is in the public interest, and
- the employee or other worker has a reasonable belief that the information showed a relevant failure (even if that belief is, in fact, incorrect)

For further information, see Practice Note: **Whistleblowing—protected disclosures**.

To qualify for protection, the qualifying disclosure must also be a protected disclosure. Since June 2013, there is no longer a requirement that the disclosure is made in good faith. However, to be protected, disclosures must be made to particular persons. This is usually the employer where the employer has a prescribed procedure dealing with such matters. Usually, companies would prefer to have the opportunity to deal with such disclosures internally first and accordingly most UK companies have introduced internal whistleblowing schemes even though this may not be required by relevant industry regulators. Subject to further qualifying conditions, disclosures may be made to a third party, such as a 'prescribed person', ie a specified industry regulator.

References:

ERA 1996, s 43A

For further information, see Practice Note: **Whistleblowing—protected disclosures**, in particular the sections entitled **When qualifying disclosures are protected** and **Prescribed persons**.

Under **ERA 1996**, employees and other workers are protected from being treated less favourably for making a qualifying disclosure even if by doing so they reveal confidential information. Employees and other workers who make a protected disclosure are protected against dismissal (employees) or suffering a detriment, eg demotion, disciplinary action, detrimental action such as receiving no pay increase or a pay reduction or no/a low bonus award as well as detrimental action such as being bullied. The detriment can be suffered after termination of employment, eg receiving a poor reference. An employee can bring a claim against a new employer, even if a qualifying disclosure is made while employed by a previous employer. Generally, and subject to early conciliation rules, protected disclosure claims must be brought within three months from the date of the detriment or dismissal. An employer is vicariously liable for the acts of its employees (subject to reasonable steps defence) and individuals can also be held personally liable under **ERA 1996**.

References:

ERA 1996, s 47B

The Department for Business, Energy & Industrial Strategy (BEIS) has confirmed that, as a result of Brexit, the UK will not be transposing the **Directive (EU) 2019/1937** (the Whistleblower Directive) into EU law (see: **LNB News 07/10/2019 41**). Depending on the terms of any exit deal reached, it may be that the UK is required to retain it. However, as UK law in its current form largely reflects the key principles underpinning the Whistleblower Directive, a radical shift in approach seems to be unlikely. For further information regarding the Whistleblower Directive, see: '*Whistleblower Directive*' below

For further general information on the UK whistleblowing regime, see Practice Note: **Whistleblowing remedies**. See also Practice Note: **Whistleblowing defences and exceptions**.

References:

Policy Statement—Whistleblowing in deposit-takers, PRA-designated investment firms and insurers

UK Corporate Governance Code (July 2018)

Financial Reporting Council: Guidance on Board Effectiveness (July 2018)

UK regulatory requirements

In the UK, there is also a requirement under the **UK Corporate Governance Code** for certain UK listed companies to demonstrate accountability in terms of appropriate risk management and internal control and for the workforce to be able to raise any matters of concern—this is often satisfied by the operation of internal whistleblowing schemes. Companies that do not comply must provide an explanation in the corporate governance statement required by the Listing Rules.

The dual UK financial services regulators have introduced additional **whistleblowing requirements** for large banks, building societies and insurers. As part of these requirements, affected firms are required to have a whistleblowers' champion and to introduce a procedure for handling all types of whistleblowing complaints. For more information, see Practice Note: **FCA and PRA whistleblowing requirements—one minute guide**.

US requirements

Following a number of high-profile financial scandals involving large companies, the US adopted SOX. Any US-listed company or a subsidiary of such a company, must provide an anonymous procedure for reporting concerns about auditing or accounting irregularities. It is unlawful for such companies to discharge, demote, suspend, threaten, harass or in any way discriminate against any employee who has reported a reasonable belief of one of the laws covered by SOX (generally, securities fraud, bank fraud, wire fraud, mail fraud, any rule or regulation of the SEC, and any federal law relating to fraud against shareholders) has been broken. The US stock exchanges on which the company's securities are traded have reflected SOX in their rules. Failure to comply may result in heavy fines or even potential de-listing. Even if not required by law, formal whistleblower policies are increasingly recognised as best practice and rewarded by law enforcement and regulatory authorities. For example, the US Federal Sentencing Guidelines provide that organisations must take reasonable steps to have and publicise a whistleblowing system (which may include mechanisms that allow for anonymity or confidentiality) for employees to report potential criminal conduct without fear of retaliation.

References:

Public Company Accounting Reform and Corporate Responsibility Act of 2002 (Sarbanes-Oxley Act 2002)

The requirements under SOX have been complemented and strengthened by the **Dodd-Frank Wall Street Reform and Consumer Protection Act 2010** (Dodd-Frank), though limited somewhat by the Supreme Court's unanimous decision in Digital Realty Trust, Inc v Somers, that Dodd-Frank's whistleblower protection provisions apply only to individuals who report securities law violations to the SEC, and do not include those who report such concerns through internal channels with their employers. Dodd-Frank has increased the protection for whistleblowers in relation to potential securities law violations and also introduced financial incentives entitling such persons, in certain circumstances, to a bounty of up to 30% of any monetary sanctions (of over $US 1million) collected by the Securities and Exchange Commission (SEC) (the regulator with primary responsible for the enforcement of SOX). During 2018, the SEC paid more than $US 268 million in whistleblower awards to 13 individuals, a larger figure than for all prior years combined. For further information, see the **SEC Office of the whistleblower website**.

References:

Dodd-Frank Wall Street Reform and Consumer Protection Act 2010

Digital Realty Trust, Inc v Somers138 S Ct 767 (2018)

With the SEC awarding such record-breaking sums and following the Digital Realty decision narrowing the availability of Dodd-Frank whistleblower protections to those reporting information directly to the SEC, would-be whistleblowers have more incentive than ever to bypass internal reporting, although the SEC has encouraged potential whistleblowers to first report their concerns internally to the company. Thus, companies need to strengthen their internal reporting procedures and create a culture within their businesses that encourages employees to report concerns internally, and seek to develop and refine robust anti-retaliation policies to encourage employees to come forward with reports of misconduct without fear of reprisal.

Requirements in other EU countries

Other European countries which have introduced some form of corporate whistleblowing requirements include Germany, Hungary, Portugal, Luxembourg, the Netherlands, Romania and Switzerland. Even where there is no such requirement, the employment rights of whistleblowers are protected in most European countries.

Generally, the requirement for companies to establish internal whistleblowing schemes in European jurisdictions is underpinned by weak sanctions. The main deterrent is public censure rather than fines and/or de-listing. On the other hand, complying with US requirements relating to such schemes (in respect of which potential sanctions are greater) creates data protection and employment risk for those companies in many EU jurisdictions.

Whistleblower Directive

A change in this landscape is likely to occur following the EU's formal adoption of the Whistleblower Directive in October 2019. In force on 17 December 2019 (and directly effective for public sector bodies), the Whistleblower Directive is the EU's response to the fragmented patchwork of whistleblowing protections that currently exist across Member States, most of which lack comprehensive frameworks.

The Whistleblower Directive, which Member States must implement by October 2021, sets down minimum standards for the protection of whistleblowers who report breaches of EU law. It grants protection to 'reporting persons', a phrase interpreted widely to include not only employees but also job applicants, contractors and former employees. It also affords protection to 'facilitators' (including colleagues and relatives) who assist the reporting person in making their disclosure.

The Whistleblower Directive includes a wide array of EU law that whistleblowers may report on, including 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.

For many Member States, the implementation of the Whistleblower Directive will lead to significant legal (and for some, cultural) changes in their approach to whistleblowers. For example, it encourages Member States to provide financial and psychological support to whistleblowers during legal proceedings, and to amend laws to prevent whistleblowers from being subject to civil claims. In addition, whistleblowers cannot be penalised for accessing the information they disclose except from where doing so it involved an unlawful act.

All companies must comply with the Whistleblower Directive's rules on retaliation, and must also guarantee confidentiality for the whistleblower's identity and the information disclosed. In addition, the Whistleblower Directive requires EU-based companies with over 50 employees or an annual turnover of €10 million to implement appropriate internal reporting channels. Such thresholds do not apply to certain specified sectors (such as the financial services sector) or companies vulnerable to money laundering or terrorist financing, for whom all rules are mandatory. Legal entities in the private sector with between 50 to 249 employees are permitted to share resources when setting up some aspects of the prescribed internal reporting mechanisms.

In order to comply with the rule on internal reporting, companies are required to:

- set up channels for receiving the reports, which are designed, set up and operated in a secure manner that ensure the confidentiality of the identity of the whistleblower and any third party mentioned in the report, and prevent access to non-authorised staff members. Such channels must allow for reporting in writing and/or orally, through telephone lines or other voice messaging systems, and upon request of the whistleblower, by means of a physical meeting within a reasonable timeframe
- acknowledge receipt of the report to the whistleblower within no more than seven days of receipt
- designate an impartial person or department for diligent following up on reports, maintaining communication, asking for further information and providing feedback to the whistleblower

Companies should also have regard to a prescribed three-tier hierarchy for reporting. In the first instance, whistleblowers are encouraged to use internal reporting channels, before turning to external channels, being:

- competent authorities (if their employer does not respond to the report within three months), and then
- publicly to the media (as a last resort or in cases of imminent danger to public interest)

However, whistleblowers will not automatically forfeit their protections if they decide to use external channels first.

The Whistleblower Directive introduces two key presumptions:

- a presumption that by disclosing the information, a whistleblower did not violate company rules on information protection, and
- (in order to bolster protection against retaliatory action and threats) a presumption that retaliatory action has occurred where whistleblowers assert they have suffered damage

In addition, the Whistleblower Directive provides a non-exhaustive list of examples of retaliatory measures.

Penalties can be imposed against those who attempt to hinder reporting, retaliate against whistleblowers, attempt to bring proceedings, or reveal the identities of whistleblowers. Any threats or attempts to retaliate against whistleblowers are also prohibited.

Each Member State must implement the Whistleblower Directive into national law, which may lead to local variations, particularly as any implementing legislation will need to be consistent with Member States' existing laws relating to criminal corporate liability and anti-money laundering.

For further information on the whistleblowing protection afforded to workers in various jurisdictions, see: **EU and International Employment Law**.

EU data protection law approach to whistleblowing

Traditionally, companies that were listed on a US stock exchange adopted compliance systems across their entire corporate group that provided for hotlines, mailboxes, or other forms of anonymous communication with their employees. Often employees of such organisations (including those in Europe) were required to make such reports if they learned of any suspicious behaviour.

This approach, however, has been challenged in various EU countries on data protection grounds, in particular in the French courts. One company was **ordered** by the French Court in September 2005 to discontinue such a whistleblowing scheme at its manufacturing plant in France. The court found that the scheme was completely disproportionate compared to the US law objectives and that the factory workers in question did not typically have access to information concerning embezzlement or accounting fraud. Further, as the policy required the employees to report on any fraud or theft, it went beyond the SOX requirements.

References:

Tribunal de grande instance de Libourne Ordonnance de référé 15 septembre 2005

The French data protection authority, Commission Nationale de l'Informatique et des Libertés, (CNIL) has also challenged such schemes. When McDonalds France sought approval for its scheme, the CNIL rejected it for various reasons including:

References:

CNIL deliberation 2005-110 26 May 2005

- the whistleblowing hotlines would create an organised system for submitting reports and collecting personal data which did not respect the fundamental rights of French employees
- by encouraging anonymous complaints, there was a greater risk of false accusations and stigma for the accused
- a disproportionate amount of data was collected and processed, and
- where employees were accused, those employees would not be informed adequately or in a timely manner about the data collected and processed

Since 2005, a company operating in France must now register its whistleblowing scheme with the CNIL. A company must either file a formal request for approval with the CNIL or, if the scheme falls within scope of the CNIL's single authorisation, it can self-certify compliance. Those matters covered by SOX fall within the single authorisation. However, CNIL's single authorisation also provides that:

References:

CNIL: Single authorisation on the use of personal data in whistleblowing schemes (in French)

- employees should not be encouraged to report on matters on an anonymous basis (anonymous reporting must be exceptional)
- the whistleblowing policy should apply only to particular categories of employees if possible
- employees should be provided with sufficient information about the whistleblowing policy
- any employee accused by a whistleblowing report should be notified by the compliance officer as soon as the accused's data is recorded, and
- any employee accused should have the right to access his/her data and request rectification or deletion
- a whistleblower's identity can only be disclosed to the judiciary after obtaining the consent of the whistleblower

On 9 December 2016, France passed the **Sapin II Law** which has amended the CNIL's single authorisation, extending whistleblowing rights to temporary and external workers, such as interns or contractors The Sapin II law has laid out a three-step process:

References:

Loi numéro 2016–1691 du 9 décembre 2016 relative à la transparence, a la lutte contre la corruption et à la modernisation de la vie économique

- whistleblowers should first speak to their supervisor or line manager about their concerns
- if the whistleblower feels there has not been sufficient action, they should go to a professional body or legal authority to raise their concerns, and

- if the authorities do not take sufficient action within three months of their concerns being raised, the whistleblower is entitled to speak publicly

Data protection authorities in France and Germany have also specifically stated that whistleblowing services present 'high risk' processing and require full Data Protection Impact Assessments to be undertaken.

In the UK, there is no requirement for the Information Commissioner's Office (ICO) to approve a whistleblowing hotline; in many other European countries, however, it is necessary to obtain approval from the relevant data protection authority before collecting and processing personal data under a whistleblowing scheme. Often, data protection authorities have been willing to give such authorisation only where certain conditions have been satisfied. For example, in Sweden one such condition is that only company executives and key employees can be reported through a whistleblowing hotline. In Hungary it is a legal requirement for the compliance officer to notify the subject of a complaint, potentially undermining the credibility of any subsequent investigation.

The **Regulation (EU) 2016/679**, GDPR came into effect in the EU on 25 May 2018. The GDPR significantly enhances the level of personal data protection and is directly enforceable in all EU countries including the UK without the need for implementing legislation. Many EU countries, including the UK, have introduced their own domestic laws to provide permitted national derogations or exceptions to the requirements of the GDPR.

References:

***Regulation (EU) 2016/679*, GDPR**

For further information on the GDPR generally, see Practice Notes: **The General Data Protection Regulation (GDPR)** and **The GDPR and DPA 2018: key data protection issues for employment lawyers**.

The GDPR gives individuals significant rights regarding their personal data. Some of these rights may potentially conflict with the public interest in protecting whistleblowers against the risk of retaliation for making a protected disclosure. For example, if employee X discloses information about employee Y to an employer and employee Y later makes a data subject access request, employee Y has a right of access to their personal data, including "where personal data are not collected from the data subject, any information as to their source" which would reveal the identity of the whistleblower. The Article 29 Working Party (now the European Data Protection Board) advises that if access is granted to a concerned individual, all the personal data of the whistleblower and any third parties should be redacted from those documents. Where this is not practicable, it may be possible to withhold the disclosure of an individual's personal data on the basis that this would interfere with the rights and freedoms of another individual. This will need to be assessed on a case-by-case and country-by-country basis in practice.

References:

***Articles 15* and *23* of *Regulation (EU) 2016/679*, GDPR**

To comply with data protection obligations, employers must ensure they adhere to strict internal procedures when handling whistleblowing cases. This should include the following steps as a minimum:

- limit the processing of personal data to that which is necessary. A whistleblower may pass on information that is irrelevant to the allegations, in which case it is the employer's or public authority's responsibility to restrict and delete any extraneous information, particularly that relating to special categories of data, to ensure that the information that is passed on is limited to that which is strictly needed for the investigation
- limit the amount of time for which the personal data is held. Once the investigation has concluded, extract the personal data held from day-to-day systems and implement technical and organisational measures to hold the personal data securely
- inform relevant categories of individuals that their personal data is being processed (where possible). For example, the whistleblower should be told, in general terms, who the possible recipients of their disclosures and personal data could be as part of the whistleblowing procedure. Informing third parties (such as regulators) may not be necessary where this would be disproportionate, so this can be assessed on a case-by-case basis

Further, in order to comply with the Whistleblower Directive, companies will soon need to prioritise confidentiality and protection of both the whistleblower's identity and the contents of the disclosure, and balance this with continued adherence to their GDPR obligations. Indeed, the Whistleblower Directive explicitly contains a reminder that any processing of personal data carried out pursuant to the Whistleblower Directive must be made in accordance with the GDPR.

Exporting personal data

Regulation (EU) 2016/679, GDPR imposes restrictions on the transfer of personal data outside the EU (and the three European Economic Area (EEA) countries of Iceland, Liechtenstein and Norway and also Switzerland and other countries deemed to have 'adequate' data protection laws), to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by Regulation (EU) 2016/679, GDPR is not undermined. The UK, on leaving the EU, will need to apply for an adequacy decision if it is not part of a withdrawal agreement.

References:

Article 44 of Regulation (EU) 2016/679, GDPR

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Regulation (EU) 2016/679, GDPR, outlined below. Where personal data disclosed through a whistleblowing scheme is to be transferred outside of the EEA, (eg to an organisation's head office which is located abroad) these data export restrictions must therefore be considered.

References:

Articles 44–50 of Regulation (EU) 2016/679, GDPR

Transfers approved by European Commission

Transfers may be made where the European Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation, ensures an adequate level of protection (referred to as 'transfers on the basis of an adequacy decision').

References:

Article 45 of Regulation (EU) 2016/679, GDPR

As at January 2019, the EU Commission has recognized Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States (limited to the Privacy Shield—see the subsection 'Transferring personal data to the US' below) as providing adequate protection. Adequacy talks are ongoing with South Korea. See the EU Commission website for up-to-date information.

Transfers subject to appropriate safeguards

An employer may also transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. Adequate safeguards may be provided for by:

References:

Article 46 of Regulation (EU) 2016/679, GDPR

- a legally binding agreement between public authorities or bodies

References:

Article 46(2)(a) of Regulation (EU) 2016/679, GDPR

- binding corporate rules (BCRs)(agreements governing transfers made between organisations within in a corporate group)

Articles 46(2)(b), 47 of Regulation (EU) 2016/679, GDPR

- standard data protection clauses in the form of template transfer clauses adopted by the Commission (see Practice Note: International transfers of personal data under the GDPR—Standard contractual clauses (Model Clauses))

Articles 46(2)(c), 46(2)(d), 93(2) of Regulation (EU) 2016/679, GDPR

- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission

Articles 46(2)(d), 93(2) of Regulation (EU) 2016/679, GDPR

- compliance with an approved code of conduct approved by a supervisory authority

Articles 40, 46(2)(e) of Regulation (EU) 2016/679, GDPR

- certification under an approved certification mechanism as provided for in Regulation (EU) 2016/679, GDPR

Articles 42, 46(2)(f) of Regulation (EU) 2016/679, GDPR

- contractual clauses agreed authorised by the competent supervisory authority, or

Article 46(3)(a) of Regulation (EU) 2016/679, GDPR

- provisions inserted in to administrative arrangements between public authorities or bodies authorised by the competent supervisory authority

Article 46(3)(b) of Regulation (EU) 2016/679, GDPR

For further details, see Practice Note: International transfers of personal data under the GDPR. Further information on international transfers is also available in the ICO GDPR guidance.

Derogations

Regulation (EU) 2016/679, GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. Those relevant to the employment context enable a transfer, or set of transfers, to a third country or international organisation to be made where the transfer is:

References:

Article 49 of Regulation (EU) 2016/679, GDPR

- made with the individual's explicit consent (unlikely to be effective in an employment context, see Practice Note: The GDPR and DPA 2018: lawful processing of personal data in employment—Lawful and specific conditions for processing—consent and explicit consent)

- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request
- necessary for the performance of a contract made in the interests of the individual between the controller and another person
- necessary for important reasons of public interest
- necessary for the establishment, exercise or defence of legal claims

The first three derogations are not available for the activities of public authorities in the exercise of their public powers.

A recital to Regulation (EU) 2016/679, GDPR indicates that transfers which can be qualified as not repetitive and that only concern a limited number of data subjects could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable and the controller should inform the supervisory authority and the data subject about the transfer. We suggest that employers are most unlikely to wish to rely on this possibility.

Regulation (EU) 2016/679, GDPR therefore limits an employer's ability to transfer personal data outside the EU where this is based only on the employer's own assessment of the adequacy of the protection afforded to the personal data.

References:

Article 49(1)(a) of Regulation (EU) 2016/679, GDPR

Article 49(1)(b) of Regulation (EU) 2016/679, GDPR

Article 49(1)(c) of Regulation (EU) 2016/679, GDPR

Article 49(1)(d) of Regulation (EU) 2016/679, GDPR

Article 49(1)(e) of Regulation (EU) 2016/679, GDPR

References:

Recital 113 to Regulation (EU) 2016/679, GDPR

Transferring personal data to the US

Historically, transfers to the US from the EU were permitted under the Safe Harbor framework, set out in the Commission Decision 2000/520/EC. However, after a reference to the Court of Justice in Maximillian Schrems v Data Protection Commissioner, the Court of Justice declared that Safe Harbor was not a valid method of exporting data (see Practice Note: International transfers of personal data under the DPA 1998 [Archived]—Safe Harbor—the invalid data export rule).

Following the demise of Safe Harbor, the EU and US authorities agreed to a new EU-US transfer framework entitled the Privacy Shield. This was approved by the Commission, which issued an adequacy decision, launching it. This decision was subsequently published as Commission Implementing Decision (EU) 2016/1250 in the Official Journal of the European Union on 1 August 2016. In October 2019, the European Commission published a report confirming its view that the US continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the EU to participating companies in the US. For further information on the Privacy Shield, see Practice Note: The Privacy Shield.

References:

Schrems v Data Protection Commissioner Case C-362/14 [2015] All ER (D) 34 (Oct)

Commission Decision 2000/520/EC

References:

Commission Implementing Decision (EU) 2016/1250

Other EU regulatory issues

As well as data protection issues, there are other regulatory hurdles for US listed companies and their subsidiaries to be aware of when implementing whistleblowing schemes which comply with SOX. Some examples are considered below.

In Germany, the requirement under SOX to have a whistleblowing scheme has attracted the attention of the employment courts. In 2005, an employment court found that Walmart had violated German employment law by implementing its scheme without first consulting with its German works council. The court found that the scheme required the pre-approval of the work council because it imposed additional burdens on employees (they could be sanctioned for non-compliance) and because the whistleblowing hotline was viewed as a mechanism for monitoring employee performance.

In other European countries (such as the Netherlands), there is also the need to obtain the prior consent of a Works Council (or employees' collective consent where no Works Council exists) before a whistleblowing scheme can be adopted.

In July 2016, a law was introduced in the Netherlands requiring companies with more than 50 employees to have a corporate whistleblowing scheme. The law defines employees widely so that it covers any self-employed persons working for the company. A regulatory body has been established called the 'House for Whistleblowers'. This body can conduct its own investigation into a whistleblowing complaint if it decides that the suspicion of abuse is sufficiently serious and well-founded. Generally, the company is required to co-operate with the House and provide all requested information or answer any questions.

Guidance from the Article 29 Working Party

The Article 29 Working Party (now the European Data Protection Board) published an opinion (**Article 29 Working Party—WP 117: Opinion 1/2006 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**) in early 2006 to provide industry across the EU with guidance in this area. It stated that:

> *'For a whistleblowing scheme to be lawful, the processing of personal data needs to be legitimate and satisfy one of the grounds set out in Article 7 of the Data Protection Directive.'*

The Working Party recognised that two potentially legitimate grounds for processing the personal data under EU data protection law were that:

- the processing is necessary for compliance with a legal obligation to which the data controller is subject (the First Ground), or
- the processing is necessary for the purposes of the legitimate interests pursued by the data controller or parties to whom the data are disclosed (the Second Ground)

The Working Party did not find the First Ground appropriate because an obligation imposed by a foreign law (such as SOX) does not qualify as a legal obligation that would legitimise data processing in the EU under Article 7(c) of **Directive 95/46/EC**, the Data Protection Directive (which has subsequently been replaced by Article 6 of Regulation (EU) 2016/679, GDPR). The Working Party found that any other interpretation would make it too easy for foreign legislators to circumvent EU data protection law.

However, the Working Party did find that the Second Ground could be potentially relied upon, as they recognised that there was a legitimate interest in ensuring the stability of financial markets and preventing fraud, bribery and financial crime. However, the Working Party found that the Second Ground required a balance to be struck between that legitimate interest and the fundamental rights of the data subject. Accordingly, it was necessary for a company to take a proportionate approach, having regard to the seriousness of the alleged offences to be notified and the consequences for the data subjects.

References:

Article 29 Working Party—WP 117: Opinion 1/2006 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

Article 6(1)(f) of Regulation (EU) 2016/679, GDPR

References:

Article 6(1)(c) of Regulation (EU) 2016/679, GDPR

References:

Article 6(1)(f) of Regulation (EU) 2016/679, GDPR

References:

Article 7(c) of Directive 95/46/EC

Article 6 of Regulation (EU) 2016/679, GDPR

Whistleblowing and data protection compliance strategy

The starting point for any compliance strategy is to have regard to the recommendations made by the Working Party in its opinion. Any industry-specific requirements (such as those applying in the banking/financial services sector in the UK) should also be taken into account. Subject to those requirements, companies should:

- instruct employees using a whistleblowing hotline to supply their own personal details on a confidential basis when making a disclosure (without prohibiting the submission of anonymous complaints)
- encourage employees to make disclosures without having to make allegations against specific, named individuals
- provide sufficient information about the scope of the hotline and how it should be used
- limit the scope of the information to be disclosed as part of the hotline (it may be better to limit this simply to corporate whistleblowing requirements such as SOX rather than widen it to cover more general wrongdoing not subject to such a procedure)

References:

Article 29 Working Party—WP 117: Opinion 1/2006 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

- inform accused employees promptly whenever a disclosure has been submitted attributing wrongdoing to them
- ensure internal procedures are in place to protect the identity of the whistleblower and the contents of the disclosure
- place a time limit on the retention of the data gathered through the hotline
- try to avoid personal data leaving the EEA (if possible) or ensuring that any necessary data transfers are lawful (such as through the use of model contractual clauses)
- ensure that the data is retained securely and protected against loss, theft or damage
- comply with any notification requirements to data protection authorities or work councils, and
- if possible, limit both the number of people entitled to report alleged improprieties and the number who might be incriminated through their use

Why data protection issues matter in whistleblowing policies

Protecting an individual's disclosure during a whistleblowing procedure in an effective way is an essential part of an organisation's internal compliance programmes. Data privacy rights play an important role in structuring the approach to whistleblowing procedures and organisations will need to take even greater care with the introduction of the GDPR, particularly given the high penalties for breaching data privacy rights.

The GDPR, particularly when it will be applied in accordance with the new requirements of the Whistleblower Directive, adds a level of complexity to internal whistleblowing procedures but the priority should be to safeguard the privacy rights of the individual with the need for a thorough and full investigation into any allegations made in order to ensure the correct procedure has been followed, which is encouraged by tough sanctions in countries like the US under SOX and financial incentives under Dodd-Frank.

Rather than being seen as a deterrent, data protection rights should create a framework within which organisations should put in place strict guidelines with handling whistleblowing requests and assist them with ensuring individuals have the best available platform to raise concerns in their organisations.

If you would like to contribute to Lexis®PSL Employment please contact:

Amy Himsworth
LexisNexis
Lexis House
30 Farringdon Street
London, EC4A 4HH

amy.himsworth@lexisnexis.co.uk
+44 (0) 20 7400 2681