# Whistleblowing — avoiding the hot water when others let off steam

***Stephanie Pritchett, Data Protection Lawyer and Consultant at Pritchetts,*** ***provides guidance for organisations seeking to bring their whistleblowing schemes into data protection compliance***

We often encourage children to report youthful misdemeanours, rather than taking their own brand of remedial measures. Sometimes, however, they need to be protected from those who might be "telling tales". A moral minefield with children perhaps: an even pricklier problem in an employment context.

Employers often set up corporate compliance whistleblowing procedures to allow employees to report, anonymously or otherwise, their concerns about potential infringements of corporate rules, or of the law, by other employees or by the organisation itself. Where such wrongdoing is taking place, workers within the organisation will often be the first to become aware of it, and are therefore likely to be best placed to 'blow the whistle'. However, those individuals may also have the most to lose if the organisation is not happy about them having sounded the alarm. The potential consequences that await whistleblowers include victimisation, loss of position or career limitation.

Organisations therefore need to create a culture in which it is safe and acceptable for employees to raise legitimate concerns. Otherwise, employees may choose to remain silent, to the detriment of all concerned, and to the benefit of those who are then protected in their dishonest or inappropriate behaviour.

To try and tackle this, organisations will often introduce whistleblowing policies which set out the procedures that will apply. Such policies may form part of a general staff policy, or a standalone policy, or may take the shape of codes of conduct which cover issues such as bribery, discrimination, harassment and general relationships between workers.

In some international jurisdictions, public companies are legally required to have policies or codes of conduct in place covering standards expected of employees. These can relate to certain financial, accounting and corporate governance matters (for example under the US Sarbanes-Oxley and Dodd-Frank legislation), meaning that many multi-national organisations will introduce standard policies and whistleblowing hotlines in all worldwide jurisdictions in which that organisation operates.

Following caselaw developments in other European jurisdictions suggesting that some whistleblowing hotlines conflicted with data protection rules, in 2006 the European body of data protection regulators, the Article 29 Working Party ('the Working Party'), released Opinion 'WP117' ('the Opinion'). (This can be found at: www.ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf.)

The Opinion gives guidance to employees on how to operate internal whistleblowing schemes in relation to accounting, auditing, anti-bribery, banking and financial crime matters, in compliance with EU data protection laws.

This article looks at data protection aspects of the operation of whistleblowing schemes from a UK perspective, and discusses some practical ways of trying to avoid breaching the Data Protection Act 1998 ('the DPA'), and considering the recommendations given in the Working Party's Opinion.

## Legal position in the UK

In the UK, the Public Interest Disclosure Act 1998 ('PIDA') protects employees, workers, contractors, trainees, agency staff and home workers (etc.) from being subjected to any detriment on the ground that they have made a disclosure about their employer, or fellow employees, where such disclosure is made:

- with the reasonable belief that there has been wrongdoing in the organisation (that must be based in the UK)

or at an international level, or there is a reasonable suspicion that it is likely to occur;

- in respect of the following: criminal offences; civil offences and breaches of the law (including negligence, breach of contract, breaches of administrative law); miscarriages of justice; dangers to the health and safety of individuals or the environment; or deliberate attempts to conceal information relating to any of these matters. PIDA applies whether or not the information concerned is confidential;

- in good faith to their employer or to the individual they believe to have overall responsibility for that matter, or to a relevant prescribed body, (for example, appropriate regulators such as the Health and Safety Executive, the Inland Revenue, the Information Commissioner and the Financial Services Authority). Wider disclosures (for example to the police, media, MPs, and non-prescribed regulators, etc.) are also protected if, in addition to the tests for regulatory disclosures, they are reasonable in all the circumstances, and they are not made for personal gain.

To gain protection under PIDA when making wider disclosures, the whistleblower must meet one of the four pre-conditions:

(i) they must have reasonably believed that they would be victimised if they raised the matter internally, or with a prescribed regulator;

(ii) there was no prescribed regulator, and they reasonably believed the evidence was likely to be concealed or destroyed;

(iii) the concern had already been raised with the employer or a prescribed regulator; or

(iv) the concern was of an exceptionally serious nature.

The usual restrictions derived from employment law on 'minimum qualifying periods' do not apply to PIDA. Further, PIDA does not protect the genuinely self-employed, volunteers, the intelligence services or the army.

Since April 2010, claimants at an employment tribunal have been able to indicate that they consent to the tribunal taking steps to notify the appropriate regulator of the relevant disclosure. This is so that even if a whistleblowing claim fails or settles, the regulator can decide whether to conduct an investigation into the disclosure that has been made.

PIDA does not require UK employers to set up formal whistleblowing procedures. However, many employers will wish to do so to ensure that they are aware of potential malpractice, wrong-doing or misconduct in the organisation; and/or so that they can take steps to minimise any adverse PR risks, or risks of the employee suffering any detriment, owing to a disclosure.

Therefore, whilst whistleblowing policies may be an attractive option for organisations, they must also be established in compliance with the DPA. This means that for whistleblowing schemes to be lawful, any personal data processed as part of the procedures must be done so legitimately, and must satisfy one of the grounds set out in Schedules 2 and 3 of the DPA. The grounds include, among others, situations where:

***"...the Working Party has concluded that an obligation imposed by a foreign legal statute or regulation does not qualify as a legal obligation that would legitimise data processing in the EU."***

**The processing is necessary for compliance with a legal obligation to which the data controller is subject:** An example of where this might be possible is in a financial services organisation with clear requirements regarding certain types of offence. It should be noted that, while it seems that this condition could theoretically include a situation where an organisation has an obligation to comply with international legislation requiring the establishment of whistleblowing hotlines (for example under the US Sarbanes-Oxley and Dodd-Frank legislation), the Working Party has concluded that an obligation imposed by a foreign legal statute or regulation does not qualify as a legal obligation that would legitimise data processing in the EU.

**The processing is necessary for the purposes of the legitimate interests pursued by the data controller, or by the third party, or parties, to whom the data are disclosed:** Here the Working Party's view is that whistleblowing schemes adopted to ensure the stability of financial markets and the prevention of fraud, anti-bribery, banking and financial crime or insider trading, might be seen as serving a legitimate interest of a company that would justify the processing of personal data. The Working Party also accepted the need for organisations to comply with the US whistleblowing regulatory framework as a legitimate interest of those organisations for data protection purposes.

However, the Working Party has reminded organisations that a balancing exercise needs to be carried out to weigh the legitimate interests of the organisation against the fundamental rights of the data subjects concerned. Therefore, organisations wishing to rely on this condition, should carry out an impact assessment, assessing and documenting proportionality and subsidiary issues, how serious the alleged offences are, any consequences for the data subjects, and whether the data subjects have been given an opportunity to object to the processing of such data about them.

*(Continued on page 8)*

## Bringing your scheme into compliance — practical tips

The points below are based on the Working Party's recommendations, as well as the author's practical experience of dealing with the issues described above.

The following are some practical steps that should be considered when introducing or reviewing whistleblowing procedures, to ensure that, so far as possible, they comply with the DPA.

**1. Ensure legitimacy, data quality and proportionality**

Employers should ensure that procedures are set up to limit the number of people allowed to report malpractice, and also those that could be incriminated by the procedures. It may help to ensure that whistleblowing schemes only operate where they are required by law, or where they are legitimate and necessary to prevent activities which may pose significant risks to workers, and/or the organisation itself. Such schemes should also operate where it is in the substantial public interest (i.e. not just for minor breaches of company policy and the like).

**2. Publish whistleblowing procedures**

Before any policy is introduced, organisations should inform workers about:

- the procedures that are to be put in place;
- why there is a need for the policy (for example, because wrongdoing is taken seriously by the organisation; the sorts of matters regarded as wrongdoing; and the opportunity to raise concerns outside the line management structure); and
- how the policy works (for example, detail on the respect for the confidentiality of staff raising concerns if desired; an explanation about the proper way in which concerns may be raised outside the organisation if necessary; and any penalties for making false allegations maliciously).

**3. Where appropriate, encourage reporting that does not identify individuals**

There may be occasions where it is appropriate to inform the organisation that there are compliance concerns without specific individuals being named, or there may be other complaint mechanisms that can be followed less formally that are not part of the formal whistleblowing scheme. Employees should be informed about such alternatives.

**4. Limit information to be collected and retained**

The type of information processed should be strictly defined and limited to accounting, auditing and related matters where that is the purpose of the whistleblowing scheme. Where internal investigations show no evidence of malpractice, the personal data should be destroyed within two months. Where malpractice is established, personal data should only be kept until the end of the investigation, legal or disciplinary proceedings, after which it should be archived in a secure manner only as necessary and for a period appropriate to mitigate future risks or liabilities.

**5. Encourage named reporting**

Where possible, organisations should discourage (without prohibiting) anonymous reporting, and instead encourage individuals making a report to provide details about themselves. Anonymity makes it difficult to investigate the alleged wrongdoing: the facts will be difficult to corroborate, and it makes it very difficult to clarify ambiguous information, or to ask for more information. Where allegations are serious, those implicated will often try even harder to identify the source of the information, and will often allege that the whistleblower acted dishonestly, or in bad faith, which may undermine the process. However, those organisations that are required to comply with US whistleblowing legislation should seek specific legal advice on compliance, as anonymous helplines may be required in such cases.

**6. Consider the confidentiality of reporters**

Where people do identify themselves in the whistleblowing report, organisations should keep their identities confidential by not disclosing their identity to others when using the information or carrying out an investigation, unless it is absolutely necessary. The Working Party points out that if a whistleblower is found to have maliciously made statements, then the incriminated individual should be made aware of the identity of the whistleblower in order that they can exercise their law rights arising under defamation law.

**7. Consider rights of incriminated individuals**

Organisations should carry out assessments to balance the rights of the person accused of wrongdoing, the person who reported the offence and legitimate needs of the organisation.

**8. Inform incriminated individuals**

Employers should ensure that incriminated individuals are told promptly about the reports that have been made, and inform them of who will see copies of reports about them, and that they have a right under the DPA to access and rectify personal data in those reports. The Working Party accepted that organisations could restrict such rights if there is a substantial risk that implementing them would prejudice the organisation's investigation. Incriminated individuals should also be informed about any complaints and rectification procedures to which they themselves may be entitled.

**9. Focus on internal management**

To help ensure security and confidentiality surrounding reports, organisations should consider setting

up an internal team dedicated to running whistleblowing schemes. Each member of that team can be asked to sign stringent confidentiality agreements in relation to information learned through participation. The Working Party further recommend that less serious complaints should be handled within the EU, and not transmitted to overseas management.

**10. Ensure data security**

Organisations should ensure that appropriate technical and organisational measures are in place to ensure the security of personal data collected through whistleblowing procedures.

**11. Ensure the compliant use of data processors**

If third party data processors are to be used to man whistleblowing hotlines, then appropriate contracts and security measures must be established to ensure compliance with the DPA.

**12. Consider transfers outside the EEA**

Where information is to be transferred outside the European Economic Area (for example, to an organisation's head office located abroad), a mechanism must be put in place to ensure that only those personal data which must legitimately be transferred outside the EEA are actually transferred. Furthermore, compliance with the Eighth Principle of the DPA should be established through the use of standard contractual clauses, Binding Corporate Rules, or the EU Safe Harbor Scheme.

**13. Ensure ICO notification entries are up-to-date**

It may be necessary for organisations to amend their Notification Register entries at the Information Commissioner's Office ('ICO'). Such entries should make it clear that a whistleblowing scheme is in operation, and how personal data are being processed as part of the scheme.

**14. Ensure multi-nationals take specialist local advice**

Numerous EU data protection regulators have taken the view that, even if whistleblowing hotlines are established outside the EEA, if they are accessible to EEA employees, or if EEA-based parts of the organisation need to be involved in the investigations, then EU data protection laws will apply.

**15. Review old and established whistleblowing schemes**

Although it may be difficult to amend existing schemes, organisations should consider reviewing older schemes which may no longer be considered compliant with EU data protection laws and regulatory guidance. As it is widely expected that the new Bribery Act 2010 will increase the number of whistleblowing claims, any existing whistleblowing policies should also be reviewed in light of this new legislation. Clearly some organisations (particularly multi-nationals) will need to weigh up the risks of non-compliance with EU data protection laws, as against the risks of not complying with other regulatory and international obligations.

## Conclusion

With the weight of numerous, and potentially conflicting regimes, an organisation may feel it is preferable to bury its corporate head in the sand, and let employees' fear of being ostracised support this Ostrich-like behaviour. However, to do so could foster a lax compliance culture, and lead to regulatory action, fines, monetary penalties and adverse PR, not to mention loss of employee and customer confidence. A shrill warning is needed. With some careful planning and some dedicated assessments, DPA compliant whistleblowing policies can be put in place to protect the organisations and the individuals within them. This may also encourage people to discuss compliance issues and resolve them, before they become a skeleton in the closet. As ever, prevention is better than cure.

UK organisations may be interested to look at the Information Commissioner's own whistleblowing policy set out at: www.ico.gov.uk/about_us/~/media/documents/library/Corporate/Notices/whistleblowing_policy.ashx

**Stephanie Pritchett**
Pritchetts
stephanie@pritchettslaw.com

Stephanie Pritchett is the leader of PDP's training session, 'Data Protection Essential Knowledge — Level 2'.

For details of the training session, visit www.pdptraining.com