Whistleblowing — avoiding the hot water when others let off steam

Stephanie Pritchett, Data Protection Lawyer and Consultant, 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 to 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 stand-alone 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 case law 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.

Following publication of the Opinion, the Data Protection Commissioner ('the Commissioner') issued his own guidance (see http://www.dataprotection.ie/docs/Whistleblower/303.htm ('the Guidance') advising data controllers to follow the guidance given in the Opinion in order to remain compliant with the Data Protection Act 1988 and the Data Protection Amendment Act 2003 ('the DPAs').

This article looks at some practical ways of avoiding breaching the DPAs when setting up whistleblowing schemes, drawing from the Working Party's recommendations.

Legal position in Ireland

Many Irish employers will wish to set up formal whistleblowing procedures, even where not legally or contractually required to do so, to ensure that they:

- are aware of potential malpractice, wrong-doing or misconduct in the organisation; and
- can take steps to minimise adverse PR risks, or risks of the employee suffering detriment or

(Continued on page 10)

(Continued from page 9)

being dismissed, owing to a disclosure that they have made.

For whistleblowing schemes to operate in compliance with the DPAs, any personal data processed as part of the procedures must be processed legitimately. This means that personal data must be collected and processed 'fairly' as required under Section 2.1(a) and Section 2D of the DPAs, and fair processing information must be made readily available to data subjects. Further, one of the 'processing conditions' under Sections 2(A) and 2(B) of the DPAs should be met. These include (but are not restricted to) situations where:

"For whistleblowing schemes to be in compliance with the DPAs, any personal data processed as part of the procedures must be done so legitimately. This means that personal data must be collected and processed 'fairly' as required under Section 2.1(a) and Section 2D of the DPAs, and fair processing information must be made readily available to data subjects."

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.

Bringing your scheme into compliance — practical tips

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 DPAs.

1. Ensure legitimacy, data quality and proportionality

The Commissioner advises organisations to consider whether they "have a good reason to put such a [whistleblowing] scheme in place, taking account of the risk to the rights of individuals that may result from its establishment." Therefore, reasons should be assessed carefully and documented before such a scheme is created. 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 a policy is introduced, the Commissioner advises organisations to consider whether they have "provided comprehensive information to employees on the operation of the scheme." 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). Workers should also be informed about the sorts of matters regarded as

wrongdoing, and the availability of opportunities 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. Alternatively, 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.

The Office of the Data Protection Commissioner ('the ODPC') has said that "whistleblowing only becomes a data protection issue when personal data are involved." Personal data are defined in the DPAs as "data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller." Data includes both automated data and manual data.

In the ODPC's view, the DPAs do not apply to whistleblowing schemes where:

- no record is kept, in either electronic or manual form, of the content of a whistleblowing report or of the person either making the report or the person who is the subject;
- a whistleblowing report relates to an irregularity in an organisation but responsibility for the irregularity is not, and cannot readily be, attributed from the content of the report.

The Guidance states that "from a data protection perspective, the best practice approach for an organisation introducing a whistleblowing scheme is to arrange, to the maximum extent possible, that the data produced from such a scheme refer to issues rather than individuals." However, the Commissioner recognises that this will not always be practical.

On the issue of whistleblowing schemes set up in compliance with the US Sarbanes-Oxley Act, the Guidance states that "as the focus is on the reporting by employees of questionable accounting or auditing matters, a whistleblowing scheme designed solely for compliance [with Sarbarnes-Oxley] does not appear to require the recording of personal data." However, it is not clear how easy it is in practice to avoid collecting personal data when complying with the Sarbanes-Oxley requirements.

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 the data 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

The Guidance states that 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 help lines 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 potential 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. Employers should also ensure that individuals are informed about 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 accepts that organisations could restrict the rights described above if there is a substantial risk that implementing them would prejudice the organisation's investigation. Incriminated individuals should also

(Continued on page 12)

(Continued from page 11)
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 recommends 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 DPAs.

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 Section 11 of the DPAs (prohibiting overseas transfers of personal data unless the country has been deemed 'adequate' for the purpose) should be established through the use of standard contractual clauses, Binding Corporate Rules, or the EU Safe Harbor Scheme.

13. Ensure that ODPC registration entries are up-to-date

It may be necessary for organisations to amend their registration entries to make it clear that a whistleblowing scheme is in operation, and how personal data are being processed as part of the scheme. Entries should include the fact of whether personal data are to be transferred to a third party outside of the EEA.

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. Consider employment law issues

The discussion in this article is confined to data protection issues arising from whistleblowing schemes. Organisations may need to seek specialist advice relating to the employment law issues that may arise in addition to the data protection implications.

16. 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. 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 assessment whistleblowing policies can be put in place to protect 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.

Stephanie Pritchett
Pritchetts
stephanie@pritchettslaw.com

Stephanie Pritchett is the trainer for PDP's practical training session, 'Data Protection Essential Knowledge — Level 2'.

For details of the training session, visit www.pdp.ie/training