EJLT European Journal of Law and Technology

Whistleblowing and data protection principles: is the road to reconciliation really that rocky?

David B. Lewis [1]

Cite as: Lewis, D. B., 'Whistleblowing and data protection principles: Is the road to reconciliation really that rocky?', European Journal of Law and Technology, Vol. 2, No. 1, 2011.

Abstract

Legislation in many countries now recognises that there is a public interest in the disclosure of wrongdoing. Not only can whistleblowers benefit their employers by offering solutions to work problems but they can play an important role in the fight against fraud and corruption. However, reporting procedures can cause problems because both whistleblowers and alleged wrongdoers may have rights as data subjects under the Data Protection Directive 95/46/EC. This article explores the areas where there might be conflicts between good practice in whistleblowing arrangements and data protection principles. It examines how the EU's Article 29 Data Protection Working Party responded to the alleged clash between the requirements of the US Sarbanes-Oxley Act 2002 and the Directive. The author concludes that, although some tensions might exist, it is fairly easy for companies to comply with both EU and US legislation. Nevertheless, he suggests that it would be helpful if the Working Party issued a revised Opinion (or the Directive was amended)in order to reflect the enormous changes in the way information is acquired and disseminated since the Directive came into effect.

1. The importance of encouraging whistleblowing and the introduction of SOX

There is no universally recognised definition of whistleblowing but the following is most commonly used by researchers: 'the disclosure by organisation members (former or current) of illegal, immoral or illegitimate practices under the control of their employers, to persons or organisations that may be able to effect action'. [2] It will be observed that this covers anonymous reporting and the use of both internal and external channels. In practice, what is most important is the definition of the circumstances in which people who disclose wrongdoing will be protected from retaliation.

An old-fashioned view of whistleblowers is that they are disloyal troublemakers. [3] A more positive approach is to regard them as dedicated people who provide an important safety net when other forms of regulation fail. Such an approach recognises that workers are often in the best position to know whether there is malpractice within an organisation. More positively, it is argued that whistleblowers can benefit their employers by offering solutions to work problems. Those who first contact their managers about wrongdoing provide them with an opportunity to correct it before the matter escalates. In the light of such general arguments, particular health and safety disasters and an increasing desire to combat fraud and corruption, [4] many countries have introduced specific legislation. A variety of approaches have been taken, with some statutes being inapplicable to private sector entities. [5] The common denominator is that these measures aim to encourage the reporting of concerns and protect whistleblowers in the public interest. [6]

Following some notorious financials scandal, including Enron and WorldCom, the US government concluded that existing federal and state legislation was inadequate. [7] As a result the Sarbanes-Oxley Act 2002 (SOX) was passed and this applies not only to US public companies (and their agents and contractors etc) but to all companies holding shares or debt securities which are registered with the Securities and Exchange Commission. [8] Section 301(4) of SOX imposes the following duty: 'COMPLAINTS. - each audit committee shall establish procedures for -(A)the receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters; and (B) the confidential, anonymous submission by employees or the issuer of concerns regarding questionable accounting or auditing matters'. To reinforce this, Section 806 of SOX makes it illegal for companies to 'discharge, demote, suspend, threaten, harass, or in any other manner discriminate against' employees for making use of these procedures or assisting government and regulatory agencies in their inquiries into accounting irregularities. Companies who fail to comply with the SOX requirements may face heavy fines and possible de-listing from the stock exchange. Subsequently the Dodd-Frank Wall Street Reform and Consumer Protection Act 2010 strengthened the legal protection for prospective whistleblowers and introduced significant financial incentives for individuals to disclose 'original information' to the regulator which leads to successful enforcement action. Significantly for our purposes, Section 929A makes clear that the SOX whistleblowing provisions (described above) apply not only to companies listed in the US but also to subsidiaries and affiliates of such companies, wherever located, whose financial information is included in consolidated financial statements.

So why did SOX cause such a stir in Europe? The answer lies in the fact that, prior to the Dodd -Frank Act 2010,many US companies treated SOX as having extra -territorial effect [9] and have introduced anonymous telephone hotlines in some countries(some of which are provided by third parties) without considering the possible impact of the Directive 95/46/EC. Nevertheless, it is not immediately obvious why the introduction of procedures that are designed to encourage employees to disclose financial irregularities should be so contentious. In the writer's opinion, what seems to have happened is that some Member States who were not particularly sympathetic to the concept of whistleblowing anyway have successfully created the impression that listed companies are compelled to have anonymous mandatory reporting hotlines. It almost goes without saying that evoking memories of mandatory denunciations in both fascist and communist regimes and

regarding informants as tools of repression can only undermine the effectiveness of whistleblowing in the fight against fraud and corruption. In fact, SOX merely requires that anonymous reporting should be an option and any duty to disclose is imposed by particular multi-nationals and not the legislation. Indeed, as we will discuss later, anonymous disclosures can be hard to investigate and mandatory reporting is difficult to enforce in practice.

2. European data protection laws and the Article 29 Working Party

In 2005 the French Data Protection Authority (CNIL) refused to allow McDonalds and Exide Technologies, two SOX -regulated multi-nationals, to operate whistleblowing hotlines. [10] It was ruled that the proposed procedures were not compatible with the French law on privacy [11] as they might deny individuals the right to know the nature of allegations as well as the opportunity to defend themselves. Undoubtedly this would be a serious matter if it were true. However, it does not follow that because an allegation is made that it is appropriate to inform the subject of it immediately. If a preliminary screening indicates that the information supplied is not credible no defence needs to be sought or offered. Indeed, in these circumstances automatically notifying the individual might cause unnecessary stress. On the other hand, if an initial investigation suggests that there is a case to answer, natural justice requires that the alleged wrongdoer should have his or her say (see below).

In January 2006 the Dutch Data Protection Board produced a recommendation on whistleblowing which essentially followed the French approach i.e. hotlines should not be used as a replacement for existing channels of communication. The following month the EU's Article 29 Data Protection Working Party [12] issued a non -binding 'Opinion 1/2006 on the application of the 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'. [13] This advisory body consists of data protection officers from the Member States and one of its tasks is to promote a uniform application across the EU of the principles contained in Directive 95/46/EC. Also in February 2006 the chairman of the Art.29 Working Party wrote a letter to the US Securities and Exchange Commission making it clear 'that EU data protection rules neither prevent companies from setting up such whistleblowing schemes nor from processing personal data reported by whistleblowers...' Nevertheless, the Working Party set some conditions and these are discussed below.

The processing of personal data inside the EU and the transfer of such data to countries outside the European Economic Area (EEA) is subject to the data principles contained in Directive 95/46/EC. This Directive imposes broad duties on those who collect personal data (data controllers), as well as providing extensive rights on individuals about whom data is collected (data subjects). Personal data is defined in Article 2(a) of the Directive as information relating to either an identified person or a person who can be identified, directly or indirectly, by a reference number or by one or more factors specific to him. The Directive has been implemented in the UK via the Data Protection Act 1998 [14] and most personnel files will be covered by it.

The Data Protection Directive 95/46/EC applies to the use of whistleblowing procedures because they are highly likely to involve the collection, registration, storage, disclosure and destruction of data related to an identifiable person. Although many whistleblowing schemes focus on the position of the discloser rather than the alleged wrongdoer, it is clear that the latter have the same rights in relation to the processing of personal data. For whistleblowing arrangements to be lawful, the processing of personal data must be legitimate and satisfy one of the grounds in Article 7 of Directive 95/46/EC. In this context, the two possibilities are that the establishment of a whistleblowing system is necessary for: (i)'compliance with a legal obligation to which the controller is subject' [15] or (ii)'the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)'. [16] In relation to Art. 7(c), the Working Party concluded that a duty imposed by foreign legislation (for example, SOX), does not qualify as a legal obligation that would legitimise data processing in the EU - otherwise it would be easy for overseas legislators to circumvent the EU Directive. However, it had no difficulty in finding that employers have a legitimate interest both in complying with the US regulatory framework and in identifying and dealing with financial misconduct [17]. The Working Party noted that the balance of interest test would take into consideration issues of proportionality, subsidiarity, the seriousness of the alleged wrongdoing that can be reported and the consequences for the data subjects. Indeed, in the context of Art.7(f), Art.14(a) of Directive 95/46/EC gives individuals the right 'to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation.'

Art.6(1)of Directive 95/46/EC stipulates that personal data must be processed fairly and lawfully; they must be collected for specified, explicit and legitimate reasons and not be used for incompatible purposes. Additionally, the processed data must be relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Finally, appropriate measures must be taken to ensure that data which are inaccurate or incomplete are rectified or erased. It is the application of the principle of proportionality that led the Working Party to recommend that companies 'should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct...whether it might be appropriate to limit the number of persons who may be reported through the scheme'. In this writer's opinion, such an approach is fundamentally misconceived. As a matter of principle, whistleblowing schemes should encourage *all* staff (and perhaps relevant outsiders) to raise serious concerns irrespective of the number or nature of the alleged wrongdoers. Indeed, empirical research in the UK shows that many employers in both the public and private sector have whistleblowing procedures that can be invoked by non -employees, for example, agency workers, contractors, sub-contractors, suppliers, customers and members of the public. [18]

More positively, the Working Party makes a strong case for identified and confidential reporting rather than anonymous disclosures. There are several weighty arguments against anonymity: (i) it is more difficult to investigate a concern;(ii) a person's identity might be guessed from the circumstances; (iii) it is easier to provide protection against reprisals if concerns are raised openly; [19] (iv) anonymity may cause people to focus on

the possible motives of the discloser rather than the merits of the message that is being conveyed. The Working Party considered that the requirement to collect data fairly means that whistleblowing arrangements should encourage confidential reporting by identified persons. Nevertheless, acknowledging the reality that serious concerns are sometimes raised anonymously, the Working Party accepted that anonymous reports should be provided for if they were regarded as a last resort and subject to conditions. Unfortunately their suggestion that the possibility of reporting anonymously should not be advertised does not make much sense. Clearly, whistleblowing policies/procedures should promote open or confidential reporting and give undertakings about protecting disclosers. They should also acknowledge that in certain circumstances confidentiality cannot be maintained, for example, where there is a legal obligation to report people to the police or other regulatory authorities. [20] However, if a potential whistleblower is not willing to be identified, surely it is better for a policy/ procedure to state that anonymous reporting is preferable to remaining silent about alleged serious wrongdoing? What is less contentious is the Working Party's advice that anonymous concerns should be dealt with cautiously and perhaps investigated more speedily because of the risk of misuse.

Given the obligations contained in Art.6 (see above), the data collected and processed through a whistleblowing procedure should be confined to information which relates to the purpose of ensuring proper corporate governance. The Working Party Opinion focuses only on financial misconduct but it acknowledges that in some Member States the law provides for other types of wrongdoing to be disclosed in the public interest. [21] Whatever the scope of the whistleblowing procedure, the personal data processed must be limited to that which is strictly and objectively necessary to verify the allegations made. It is also recommended that 'complaint reports should be kept separate from other personal data'. [22] In this context it is worth referring to the detailed guidance contained in Paragraph 5.9 of the UK Whistleblowing Arrangements Code of Practice: [23] 'As many whistleblowing concerns will be raised with and addressed by line managers in the course of day -to -day business, care should be taken not to impose a disproportionate scheme for recording all whistleblowing concerns. It should be sufficient for managers to record and pass on a summary of the concern where an employee has formally invoked the whistleblowing policy, or where the manager thinks the concern of such significance that it is sensible that a central record is kept. Those who receive a concern outside of line management - be it a designated officer or an internal hotline - should keep records and these should also be logged centrally…..The organisation should ensure that the compilation and maintenance of these records complies with its data protection procedures'.

According to Art.6 of the Directive, personal data should be kept for the period of time needed for the purpose for which it has been collected or for which it is further processed. The Working Party recommended that personal data processed under whistleblowing arrangements should usually be deleted within two months [24] of an investigation being completed and personal data relating to unsubstantiated allegations should be deleted promptly. [25] However, if disciplinary or legal action is taken either against the alleged wrongdoer [26] or the whistleblower (in cases of malicious reporting), personal data will need to be retained until the conclusion of the proceedings and the period allowed for any appeal. It is worth commenting here that many employers would prefer to keep

information until they are sure that a whistleblower is not going to claim that they were victimised for making a disclosure [27] or that their concern was not adequately investigated.

Art. 10 of the Directive requires the data controller to inform data subjects about the existence, purpose and functioning of a whistleblowing procedure, the potential report recipients and the right of access, rectification and erasure for those who are the subject of allegations. Such communications will also provide the controller with an opportunity to emphasise that confidentiality will be maintained as far as possible and that those who abuse the system may be punished. Art.11 requires people to be told when personal data is collected from a third party. Thus the subject of an allegation should be informed as soon as practicable after the data about them has been recorded. This would seem to be the case even if the recipient of the information believes the information to be totally false. A more commonsense approach might be for an organisation to state explicitly in its whistleblowing arrangements that individuals will only be notified about false allegations if there is reason to believe that they were made maliciously. The Working Party recommends that where there is a real risk that such notification would undermine the employer's ability to investigate the concern effectively or obtain the necessary evidence, notification to the suspected wrongdoer should be postponed for as long as the risk remains. Although Art. 12 of the Directive provides a data subject with the opportunity to have access to personal data in order to check its accuracy and to rectify it if necessary, Art.13 stipulates that these rights may be restricted in order to protect 'the rights and freedoms of others'. It logically follows that if potential whistleblowers are to be assured of confidentiality the alleged wrongdoer's right of access will have to be curtailed.

Art.17 requires the data controller to take all reasonable technical and organizational measures to preserve the security of the data. The aim is to protect it from accidental or unlawful destruction or accidental loss and unauthorised disclosure or access. Reports of wrongdoing can be collected by any data processing means and the Working Party recommends that 'such means should be dedicated to the whistleblowing system in order to prevent any diversion from its original purpose and for added data confidentiality.' Where the whistleblowing procedure consists of a hotline operated by an external provider, the data controller must take all the measures necessary to guarantee the security of the information throughout the whole process. Since the third party provider will act as a data processor, companies should ensure that a contract is drawn up which specifically deals with the security of data. Significantly, page 15 of the Opinion makes it clear that the Working Party prefers in -company whistleblowing schemes to external provision. It suggests that a specific organisational unit should be established to handle reports of wrongdoing and lead investigations. This would consist of a limited number of specially trained and dedicated people who are strictly separated from other departments, including human resources. Where an external provider is used, the Working Party suggests that it should communicate the information processed only to the persons specified as being responsible for the investigation or for taking the measures necessary to follow up the facts reported.

The Working Party acknowledges that the nature and structure of multinational businesses mean that information about alleged wrongdoing may need to be disseminated outside the EU. As a matter of principle, the Working Party stated that multinationals should deal

with reports in one country rather than share the information with other companies in their group. However, in certain circumstances dissemination within the group may be necessary as part of the investigation or if the alleged wrongdoing results from how the group is structured. Articles 25 & 26 of Directive 95/46/EC apply where personal data is transferred to third countries. According to the Working Party, where the third country to which the data will be sent does not ensure the level of protection required by Art.25, data can be transferred if the following circumstances apply: '(1)where the recipient of personal data is an entity established in the US that has subscribed to the Safe Harbor Scheme; (2)where the recipient has entered into a transfer contract with the EU company transferring the data by which the latter adduces adequate safeguards, ...(3) where the recipient has a binding set of corporate rules in place which have been duly approved by the competent data protection authorities'. [28]

3. The impact of the working party opinion in the UK

Section 3.6 of the 'Whistleblowing Arrangements Code of Practice' [29] discusses the key issue of anonymity and data protection and its first paragraph draws attention to the fact that anonymous reports can made other than via a hotline, for example, by letter or emailing/telephoning from a public place. [30] Importantly, the drafters of the Code of Practice concluded from their communications with the Art.29 Working Party that the latter's Opinion is not intended to apply to whistleblowing arrangements which do not promote [31] anonymous reporting. Additionally, correspondence with the UK Information Commissioner's Office also revealed that this data protection authority is mainly concerned about procedures which actively encourage anonymous reporting. Thus the Code of Practice suggests that

> 'Companies obliged to comply with both EU and US legislation may decide either (a) to operate a scheme that is built on open and confidential whistleblowing ... while additionally providing an anonymous mailbox or phone line, or (b) to run one scheme but with additional safeguards and procedures for handling anonymous reports'.

4. What should be in a revised directive or working party opinion?

Although the 2006 Opinion has not been fully followed in the UK, it has had more influence on other EU data protection authorities. While all Member States have transposed Directive 95/46/EC, their data protection laws are unique in some respects, especially in their application to whistleblowing arrangements. Given the importance of whistleblowing in combating fraud and other forms of wrongdoing, a strong case can now be made for a revised Directive which deals with the relationship between whistleblowing and data protection rights. As Rand Europe state in the Preface to their 'Review of the European Data Protection Directive' [32]: 'the Directive must remain valid in the face of new challenges, including globalisation, the ongoing march of technological capability and the changing ways that data is used'. There can be little doubt there has been a dramatic

global increase in the processing of data about alleged wrongdoing since the Directive came into force. At the very least the Article 29 Working Party should provide a definitive Opinion which deals with the application of data protection rules to whistleblowing on both financial and non-financial matters. [33]

To ensure that it has a direct rather than indirect impact, it is suggested that any new measure should be aimed at data controllers rather than the EU data protection authorities who would then interpret and apply it in their own national contexts. One possibility is that a revised Directive or Opinion might encourage companies to set up procedures that enable people to raise concerns without necessarily having to make allegations against named individuals. It is also critical that any revised Directive or Opinion makes it clear that hotlines should be used to supplement rather replace existing communication channels at the workplace i.e. that it is preferable to disclose information to line managers, union or other worker representatives, health and safety committees, works councils etc. Indeed, it is important that guidance is provided about the difference between help lines, internal and commercial hotlines [34] and in this respect the definitions contained in the UK Code of Practice are useful. [35] One great benefit of establishing helplines which provide free, independent and confidential sources of advice is that the data protection implications of raising a concern can be explained to a potential whistleblower before any disclosure is made.

A revised Directive or Opinion might also emphasise that the privacy of both the whistleblower and the alleged wrongdoer can best be preserved by maintaining confidentiality. However, this requires disclosers to have sufficient faith in the organisation's ability to conceal their identity and to protect them from retaliation if they are exposed. We have already outlined some of the practical arguments against anonymous reporting, yet it is also worth observing that it gives the recipient considerable power over what happens to the information. A decision to ignore or conceal cannot questioned by the anonymous discloser and presumably others are unaware that a report has been made. Contrary to the Working Party Opinion, the writer believes that the possibility of anonymous reporting internally should be advertised. However, it is must be made clear that it is undesirable in principle and should only be used as a last resort. External anonymous reports cause particular data protection problems for their recipients. Whereas regulators [36] are likely to process any credible data received and notify the data subject if there is evidence of wrongdoing, the media may take a rather different approach. [37] Indeed, in order to protect their sources and avoid data protection duties, journalists may not make any record of the initial information received. Even where an investigation supports the allegations made, journalists may not feel morally obliged to notify an alleged wrongdoer before the story is published for fear of undermining a scoop. It would be useful if a revised Working Party Opinion used the problems arising from media reporting to reinforce the case for employers having internal whistleblowing/confidential reporting procedures which nominate suitable external recipients who can be used if a person insists on disclosing information outside the organisation.

Similarly, it might be helpful if the Working Party pointed out that outsourcing hotlines can create risks and that this too makes in-house provision preferable. Data security is not the only issue here as the external routing of information may delay vital corrective action

being taken. Another important factor that militates against the use of third parties is the need to enter contractual arrangements which ensure compliance with data protection laws. In order to counter the argument that specialist external providers are attractive because many employers lack relevant expertise in handling reports of wrongdoing, detailed guidance on how to establish in-house whistleblowing procedures would be highly desirable.

One consequence of a revised Directive or Working Party Opinion covering whistleblowing about non-financial matters is that it would totally undermine the naïve suggestion that the number of people who can report or be the subject of disclosures should be restricted. It would also be less feasible for employers to handle allegations of wrongdoing via a specific organisational unit consisting of a limited number of specially trained and dedicated people. Indeed, paragraph 4.4.1 of the UK Code of Practice suggests that staff should be encouraged to raise concerns with their immediate line manager and that in large organisations there should two internal levels as alternatives:

> 'At the second tier, it might be one or more trusted individuals, the key specialist functions, or divisional or regional managers. At the top level, it could be an internal hotline or the Finance Director, the Group lawyer and/or a non-executive Director.'

Another important recommendation that should be made in a revised Opinion is that reporting should not be mandatory. [38] Apart from the serious cultural objections that arise from historical experience, a duty to disclose information about wrongdoing causes immense practical difficulties. One consequence might be that workers raise concerns when they have inadequate evidence because they fear that they might be accused of failing to perform a legal duty. In terms of enforcing an obligation to report, employers would need to establish precisely when a person acquired knowledge of wrongdoing. In addition, the principle of consistency of treatment [39] would require employers to investigate whether other employees also possessed similar evidence of wrongdoing. Unsurprisingly, many organisations feel that such efforts would not be a good use of time or resources. Not only would focussing on the actual or potential disclosers distract attention from the message but it is hardly conducive to harmonious industrial relations.

Next we turn to the issue of data transfers outside the EU. We have already mentioned that in order to comply with EU law, transfers of information, including that from an outsourced hotline provider, must meet the 'safe harbor' requirements. [40] Given that the Organisation for Economic Co-operation and Development emphasises the principle of free flow of data between its member countries, it could be argued that attempting to regulate transfers of data to a third country is inappropriate in today's society. Indeed, one effect of electronic networks is that they facilitate the dissemination of information globally, which means that personal data published in the EU will be accessible externally. Not only is it unnecessary to distinguish between EU and non -EU countries but it may also be counter-productive - obligations which are thought to be excessive or ineffective may well be disregarded in practice and thus bring the EU Directive into disrepute. [41] Arguably the worst possible scenario is that data controllers become subject to conflicting legal duties in a situation where it is unclear which laws take precedence. Such a scenario clearly arose where SOX required anonymity to be preserved and the Directive was interpreted by some

as requiring whistleblowers to be identified. However, in the writer's opinion a sensible interpretation of the existing Directive makes US and EU law compatible. Nevertheless, it would be preferable if Directive 95/46/EC were amended to make clear that lawful publication in a Member State will not amount to a breach of Articles 25 & 26. [42] Clearly this would go a long way towards dealing with the problems caused by the extra -territorial effect of SOX.

5. Conclusion

Whether and how the Data Protection Directive is amended (or the Working Party Opinion revised) may well depend on any future decision about the introduction whistleblowing legislation across the EU. Given the general recognition that confidential reporting can be an extremely useful tool in combating corruption and fraud, [43] the European Commission may be willing to promote such legislation. If this does occur, it would provide a golden opportunity to emphasise that individual data protection rights cannot always be paramount [44] and that it is vital to the health of democratic societies that people are encouraged to disclose serious wrongdoing and are adequately protected if they do so.

In the short term it might be useful if the national data protection authorities in Europe provided detailed practical guidance on the inter-relationship between freedom of expression, freedom of information and privacy rights. This could then be used by employers to explain to their staff the possible implications of the organisation's whistleblowing arrangements. Such guidance would be particularly timely in the UK given that Section 7 of the UK Bribery Act 2010 makes the failure by a commercial organisation to prevent bribery a criminal offence but it is a defence to prove that there were in place 'adequate procedures designed to prevent persons...undertaking such conduct'. Under Section 9 of this legislation, what will constitute an adequate procedure will be set out in guidance to be published by the Secretary of State. However, it is already clear that the new Bribery Act puts more pressure on employers to establish effective whistleblowing arrangements. [45]

Although most countries do not require employers to have whistleblowing/confidential reporting procedures, [46] there are very good reasons to have them. Apart from the principle of promoting a communications culture and the practical benefit of facilitating the early rectification of wrongdoing, there is a major legal advantage. Put briefly, if an effective internal procedure exists, it is more difficult for workers to argue that an external disclosure was reasonable. [47] In the writer's opinion it would be good practice for employers to introduce both data protection arrangements and confidential reporting procedures but they should do so only after extensive consultation with staff [48] and negotiations with union or employee representatives. [49] Such agreed procedures might: gain publicity through the bargaining process and be formally communicated via personal messages, the intranet etc in order to promote awareness; provide for education and training [50] about their use which might reassure workers that a suitable balance between privacy and freedom of speech at the workplace has been achieved; ensure that independent advice and feedback [51] are available; facilitate the representation of both discloser and alleged wrongdoer; ensure that action is taken to deal with proven wrongdoing and that the arrangements are monitored regularly and amended when

necessary. [52]

---

[1] David Balaban Lewis is currently Professor of Employment Law at Middlesex University, England. The views expressed in this article are the author's own and do not reflect those of his employer or the organisations with which he is connected.

[2] Near, J. & Miceli, M. 1985. 'Organizational Dissidence: The case of whistle-blowing',*Journal of Business Ethics.* 4:1,1-16

[3] Lewis, D. 2011 'Whistleblowing in a changed legal climate: is it time to revisit our approach to trust and loyalty at the workplace?' 2011 Business Ethics: a European Review 20:1,71-87

[4] See: Carr, I and Lewis, D 2010 "Combating Corruption through Employment Law and Whistleblower Protection".Industrial Law Journal. Vol. 39 No.1 pp 1-30

[5] See: Lewis,David 2001 'Whistleblowing at work: on what principles should legislation be based?' Industrial Law Journal Volume 30 No.2 pp 169-193.

[6] For example, the UK, US, Ghana, New Zealand, Australia, South Africa, Norway and Japan. On the recent state of play in Europe see The Council of Europe Resolution 1729 entitled 'The protection of whistleblowers'(April 2010) and accompanying Recommendation 1916 which has the same name. Available at http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta10/EREC1916.htm and http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta10/ERES1729.htm

[7] See: Dworkin, T. 2007 'SOX and Whistleblowing' 105 *Michigan Law Review* 1757-1780

[8] Over 1000 foreign companies list their securities in the US and voluntarily subject themselves to US laws.

[9] In *Carnero v Boston Sci Corp, 433 F3d 1 (1st Cir 2006), 126 S Ct 2973 (2006)*, the First Circuit held that section 806 of SOX does not protect a foreign citizen who reports accounting irregularities at a US corporation's foreign subsidiary. By way of contrast, in *Walters v Deutsche Bank AG, 2008-SOX-70* (ALJ Mar. 23, 2009) it was decided that this section protected a complainant who worked in Switzerland for a Swiss subsidiary of a foreign, publicly traded parent company covered by SOX. For a detailed discussion about the external impact of SOX see: Dowling, D: 'Sarbanes - Oxley Whistleblower Hotlines Across Europe: Directions Through the Maze'. 42 *The International Lawyer.*2008.

[10] *McDonald's, CNIL Délibération No 2005-110, May 26 2005* and *CEAC/Exide Technologies, CNIL Délibération No 2005-111, May 26 2005*).

[11] Law No.78-17 of January 9th 1978 (as amended).

[12] The Working Party was established under Article 29 of Directive 95/46/EC and its role is described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

[13] 00195/06/EN. Working Paper 117. The timing of the Opinion suggests that the Working Party was keen to achieve a harmonised European position and to avoid the situation where data protection authorities in the Member States took divergent

approaches. To some extent they have been successful in this, the UK being a notable exception (see below).

[14] Other relevant UK legislation on data protection includes: Human Rights Act 1998 ;Freedom of Information Act 2000; Regulation of Investigatory Powers Act 2000; Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699); Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/2905). In 2005 the Information Commissioner issued ' *The employment practices code*'. (Wilmslow: Information Commissioner's Office.) and in May 2009 the British Standards Institute published the first British Standard on personal information management (*Data protection: specification for a personal information management system*. BS 10012:2009. London: BSI.)

[15] Article 7(c)

[16] Article 7(f)

[17] In the writer's opinion, the same argument would apply to other forms of serious wrongdoing at the workplace.

[18] See: Lewis, D 2006 "The contents of whistleblowing/confidential reporting procedures in the UK: some lessons from empirical research".Employee Relations. Vol.28 No.1 pages 76-86

[19] For example, Part IVA of the UK Employment Rights Act 1996 (ERA) only protects identifiable workers.

[20] For example, in relation to money laundering or acts of terrorism.

[21] For example, the definition of a 'qualifying disclosure' in Part IVA Employment Rights Act 1996 covers an extremely wide spectrum of wrongdoing, ranging from criminal acts or omissions causing extreme public harm to technical breaches of contract that only affect one individual.

[22] Opinion page 12

[23] PAS 1998: 2008. British Standards Institute. This document was developed to be of assistance in all sectors but page viii states that it 'is not to be regarded as a British Standard'. Thus compliance 'does not of itself confer immunity from legal obligations'.

[24] It is not made clear why this period has been chosen.

[25] It is interesting to note that in its policy statement entitled 'Whistleblowing, the FSA and the Financial Services Industry' (2002), the Financial Services Authority stated that it taped most calls and kept confidential written records for three years.

[26] According to the Data Protection Act 1998 Section 2(g), personal data consisting of the commission or alleged commission of any offence by the data subject amounts to sensitive data. Paragraph 2(1) of the Schedule to the Data Protection (Processing of Sensitive Personal Data) Order 2000. S.I. 2000/417 allows processing if it (a) is in the substantial public interest; (b) is necessary for the discharge of any function which is designed for protecting members of the public against-(i) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person, or (ii)

mismanagement in the administration of, or failures in services provided by, any body or association; and (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the discharge of that function.'

[27] Part IVA of ERA 1996 requires complaints to be lodged with an employment tribunal within three months of the detriment/dismissal occurring unless it is not reasonably practicable for the worker to do so.

[28] The Safe Harbor principles apply to the export of personal data to self -certified organisations. See also the*Data Protection Directive Proposals for Amendment made by Austria, Finland, Sweden and the UK*. 2002. www.dca.gov.uk/ccpd/dpamend.htm

[29] See note 23 above.

[30] It should be remembered that SOX does not require companies to have telephone or computer hotlines in place so employers can meet the requirement to have a procedure in any way they see fit.

[31] It is not entirely clear what is meant by 'promote' here. There is a difference between 'not encouraging' and 'discouraging'

[32] Prepared for the UK Information Commissioner's Office in 2009.

[33] For example, the relevant guidelines in Germany deal with violations of ethical conduct and environmental and human rights legislation. See the report entitled *Whistleblowing - Hotlines: Internal Warning Systems and Employee Data Protection* which was adopted by the working group of local data protection authorities (the *Düsseldorfer Kreis*) in April 2007.

[34] The prevalence of both internal and external hotlines in the UK is discussed in Author (with Kender,M): 2010

[35] Paragraph 3.7 states that: 'As the purpose of a helpline is to provide a safe haven where the employee can confidentially discuss whether and how best to raise a whistleblowing concern, the information and advice provided on a helpline are confidential between the helpline provider and the employee'. Paragraph 2.6 defines an internal hotline as 'facility within an organisation to which an employee can report, normally by telephone, email or web -based, a whistleblowing concern to a designated officer or function or someone senior in the organisation'. Paragraph 2.8 defines 'commercial hotline' as 'external reporting facility similar to an internal hotline that passes reports back to a senior or designated officer in the organisation.'

[36] Section 43F ERA 1996 refers to prescribed persons and these are listed in the Public Interest Disclosure (Prescribed Persons) Order 1999 (as amended).

[37] It almost goes without saying the media may be more concerned with what is of interest to the public rather than what it is in the public interest to expose. Often the media can only draw attention to wrongdoing and are not in a position to ensure that it is dealt with by the persons responsible.

[38] See generally: Tsahuridu, E & Vandekerckhove, W. 2008. Organisational whistleblowing policies: making employees responsible or liable', *Journal of Business Ethics*, 82:1,107-118

[39] This is not only good practice but unfair dismissal case law suggests that consistency is required if employers are to act reasonably.

[40] Data transfers outside the EU are less likely to be problematic if the transfer is internal to the organisation.

[41] The Rand Europe review of the Directive (see note 31) identified as a main weakness that 'The rules on data export and transfer to third countries are outmoded' and recommended that it should be easier to use Binding Corporate Rules to legitimise such transfers.

[42] See paragraph 26 of the *Data Protection Directive Proposals for Amendment made by Austria, Finland, Sweden and the UK*. 2002 (note 28 above).

[43] Article 33 of the UN Convention on Corruption 2003 provides: 'Each State Party shall consider incorporating into its domestic legal system appropriate measures to provide protection against any unjustified treatment for any person who reports in good faith and on reasonable grounds to the competent authorities any facts concerning offences established in accordance with this Convention.' See also the Council of Europe Criminal Law Convention on Corruption 1999 and its Protocol of 2003.

[44] According to paragraph 3 of the *Proposals for Amendment made by Austria, Finland, Sweden and the UK*. 2002 (see note 28 above):'The purpose of data protection rules is not to prevent the processing of personal data. Rather, it is to ensure the proportionate regulation of such processing'.

[45] For a long time the writer has held the view that all employers should have a statutory duty to establish and maintain a whistleblowing procedure. See Author 1995.

[46] In Europe, Norway is a notable exception.

[47] See for example, Sections 43G and 43H ERA 1996

[48] Paragraph 4.2 of the UK Code of Practice on Whistleblowing Arrangements (see note 22) identifies the issues that might be covered during consultation.

[49] It is worth noting that in the Wal-Mart case a German Labour Court ruled that the company violated the Works Constitution Act 1972 by unilaterally implementing a whistleblowing system without prior negotiations with worker representatives: *Wal-Mart,* Wuppertal Labour Court, 5th Div., 5 BV 20/05.June 15, 2005. Thus labour laws were regarded by some US multinationals as providing another obstacle to operating confidential reporting procedures in EU member states.

[50] These are explicitly mentioned by the British Standards Institute in *Data protection: specification for a personal information management system*. BS 10012:2009. London: BSI

[51] Paragraph 4.6 of the UK Whistleblowing Arrangements Code of Practice states that:' It should, however, be made clear that while the organisation will give as much feedback as it properly can, due to the legal obligations of confidentiality it owes to other employees, it might not be able to freely provide feedback on the outcome of any disciplinary action taken against another employee. Where this is the case, it can be particularly important that the organisation makes it clear to all those involved that the employee was right to raise the concern.' Empirical research shows consistently that a

major reason for not reporting wrongdoing is that people feel that it will make no difference: see, for example, Brown, A.(Ed).2008. *Whistleblowing In The Australian Public Sector*. Canberra: Australian National University. Communicating generally to the workforce about outcomes might encourage people to raise concerns.

[52] Paragraph 6.1 of the UK Code of Practice recommends that a review should consider the following four key elements of good practice identified by the Committee on Standards in Public Life:'(i) Ensure that staff are aware of and trust the whistleblowing avenues(ii) Make provision for realistic advice about what the whistleblowing process means for openness, confidentiality and anonymity(iii) Continually review how the procedures work in practice(iv) Regular communication to staff about the avenues open to them' Paragraph 6.8 suggests that the key findings from a review should be communicated to staff and Table 1 provides a review checklist. Similarly auditing and review are recommended by the British Standards Institute in *Data protection: specification for a personal information management system* BS 10012:2009. London: BSI