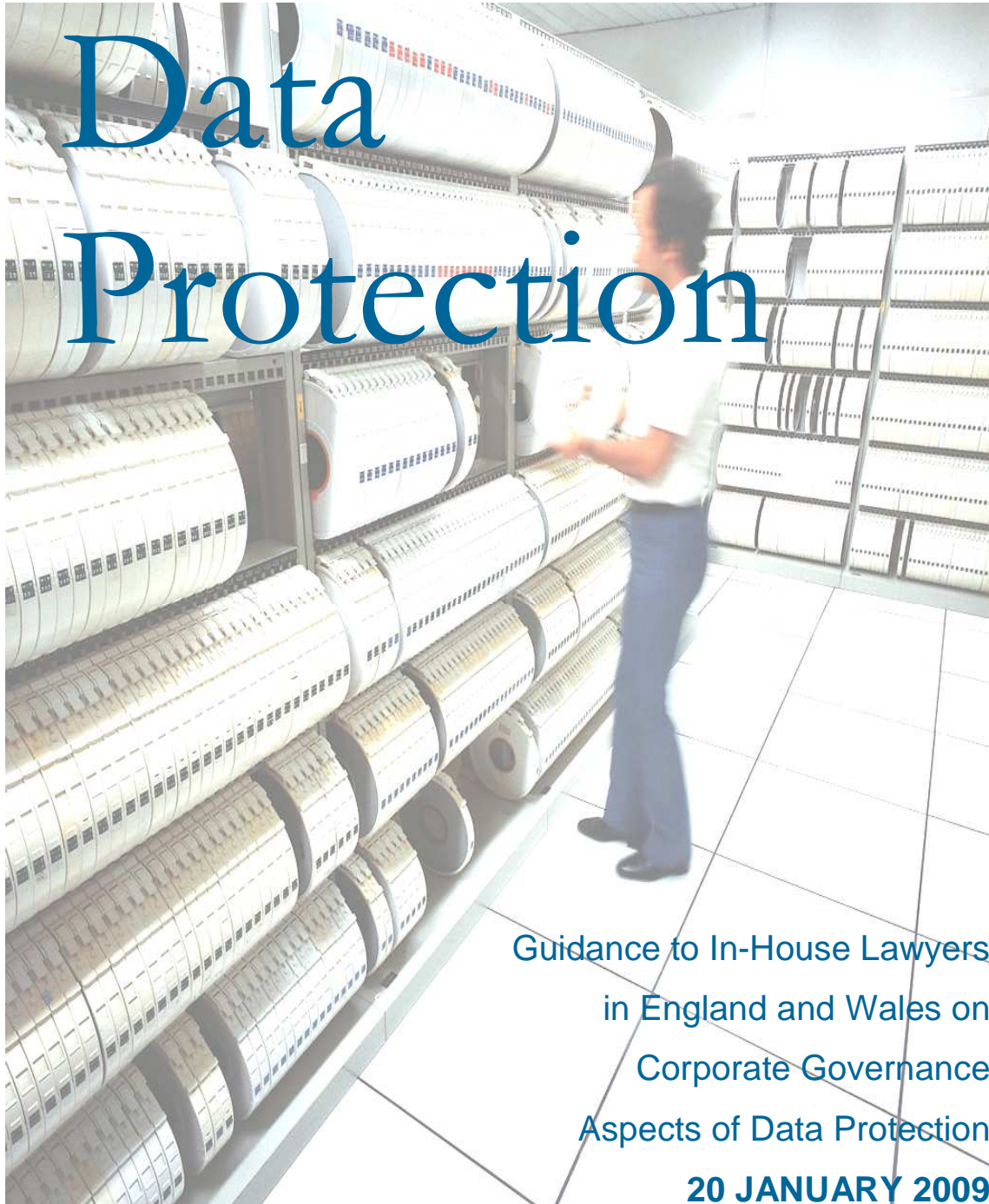




Commerce
& Industry Group recognised by The Law Society

www.cigroup.org.uk



Data Protection

Guidance to In-House Lawyers
in England and Wales on
Corporate Governance
Aspects of Data Protection
20 JANUARY 2009

Table of Contents

	Foreword	2
A.	Introduction	3
B.	What is Data Protection?	4
C.	Specific Data Protection Issues	7
D.	Governance for Data Protection	12
E.	Future Directions	16
F.	The In-house Lawyer's Role	18
	Acknowledgements and Disclaimer	21

Foreword

In this set of guidelines we look at the topic of data protection.

Three recent cases serve to illustrate that how an organisation deals with individuals' personal information can severely impact on its reputation and customer and employee confidence:

- H.M. Revenue & Customs (HMRC) lost two computer discs containing the personal details of 25 million child benefit recipients. The story was front page news and the former HMRC Director General was forced to write a personal apology to 25 million customers.
- A well-known insurance company was fined £1.26m by the Financial Services Authority (FSA) after customers lost £3.3m through identity fraud. The FSA said the company had "...let down its customers by not taking reasonable steps to keep their personal and financial information safe and secure".
- A high street bank's credit card subsidiary sent the wrong statements to the wrong people. The firm blamed a processing error at its printer for the fact that thousands of customers received statements with the correct front page but subsequent pages from someone else's account. It had to send corrected statements and a letter of apology to affected customers.

The Information Commissioner has recently recommended a number of steps that organisations should take in order to improve their data protection governance and has asked the Government to give him greater investigation, audit and enforcement powers. The Government has accepted these recommendations and is likely to

sponsor legislation in the near future, to implement them.

We think that it is especially important in the current recession, when management focus will inevitably be drawn from strategy, process and compliance to more immediate and tactical considerations to remind in-house lawyers of the importance of data protection for an organisation, to inform them of current trends in risk management and corporate governance in this area, and to provide guidance on how in-house lawyers can help their organisations establish and maintain a robust data management framework.

This guidance relates to English and Welsh law only. Specialist and independent legal advice should be taken before taking or refraining from any action as a result of the guidance contained in this document.

In order to ensure that our guidelines reflect the views of our in-house lawyer members, please let us know what you think. Please contact us through the C&I Group website www.cigroup.org.uk.

The C&I Group Corporate Governance Committee

A. Introduction

A.1 The corporate governance background

All organisations, whether public or private, rely on information about clients, competitors, employees, suppliers, debtors, creditors and stakeholders. Loss of information, fraud (especially identity fraud) and data leaks or misuse represent major security and reputational risks.

Data protection is a key governance issue and responsibility starts with the board and senior management. Policies and procedures for dealing with personal data should be established and followed throughout the organisation. A culture of fair processing and information security should be instilled, and this awareness should flow down through the various departments within the organisation to the individual employees who handle personal data on a daily basis.

Apart from legal requirements, proper collection and use of personal information makes good business sense. Sending out incorrect information to customers, losing customer information, or gathering and keeping inappropriate information about employees, not only damages an organisation's reputation but may result in the commission of an offence, the imposition of penalties or fines, and liability to pay compensation to affected individuals.

A.2 One company's experience

An employee took a company laptop home on the weekend to catch up on some work. The employee's house was burgled and the laptop stolen. The employee reported the theft. It later emerged that the laptop contained personal information on thousands of individual customers.

The organisation (which was regulated by the FSA) was found to have failed to "manage or monitor downloads of very large amounts of data onto portable storage devices", which meant it had limited control over information held in this way or how it was used, increasing the risk that it could be used to further financial crime.

It had failed to "ensure that it had effective systems and controls to manage the risks relating to information security, specifically the risk that customer information might be lost or stolen". The organisation was fined almost £1 million and had to write to all its customers apologising for the incident.¹

As it happens, this incident was dealt with by the FSA as a breach of the FSA Rules rather than the data protection rules. However, it illustrates the importance to an organisation of complying with its data protection obligations.

A.3 The role of the in-house lawyer

From advising the board on how to implement and maintain good information management practices in the context of the legal and regulatory requirements, to dealing with complaints and breaches, the in-house lawyer can play an important role in influencing good data protection practice in an organisation's information management system. The lawyer's role can be challenging in this context due to the number of other functions involved in information management, each with conflicting priorities and resource challenges that will not necessarily be fully aligned with national regulatory requirements.

¹ FSA Final Notice dated 14 February 2007

B. What is Data Protection?

B.1 Basic concepts

The Data Protection Act 1998 (DPA) (which implements European Directive 95/46/EC) governs the processing of information relating to individuals in the UK, and sets out how such information may be obtained, held, used or disclosed. It also gives individuals certain rights with regard to information about them which is held by organisations.

The DPA is overseen by the Information Commissioner's Office (ICO), an independent public body. The DPA is based on broad principles which are open to differing interpretations with differences existing at the time of publication between court decisions and ICO recommendations. This means that the in-house lawyer has to be informed about current law as well as current policy and has to provide informed guidance to the business which takes account of likely future trends in the law – especially where long term investment decisions are being made (such as on IT infrastructure).

The ICO has published extensive guidance on how the DPA should be interpreted and applied in practice, and this guidance can itself be the subject of extensive consultation with, and comment from, different interest groups. The ICO website (www.ico.gov.uk) is a very useful starting point for any DPA queries and for gathering further information on this area. The ICO also operates a helpline for enquiries about the DPA, which can be a useful source of free advice. The ICO appears more aligned at present on certain aspects of data privacy law with other European Data Privacy authorities than with recent English case law. The headline data protection case of *Durant v Financial Services Authority* [2003] EWCA Civ 1746, provides guidance on whether

data fell within a “relevant filing system” and was required to be released following a request from an individual. The case restricted the definition of personal data further than has been seen in other EU member states, and has been a matter for controversy ever since.

The DPA covers “*personal data*” - data which identifies a living individual – which is processed by equipment or is recorded in a structured, readily-accessible filing system. The DPA also contains special protections for “*sensitive personal data*” – information about a person’s racial or ethnic origin, political opinions, religious beliefs, membership of a trade union, health, sexual life or any criminal allegations, proceedings or record.

Determining what constitutes “*personal data*” is not always easy. Indeed, as mentioned above, UK and European interpretations have differed. The ICO has issued detailed guidance on what should fall within the definition². However, as the classification is open for debate, it is wise for companies to adopt a wide definition to ensure compliance (although a narrower meaning can be argued for when faced with an overly extensive Subject Access Request (see section C.2.5 below)).

It is important to understand whether your organisation is a data controller or data processor, as they have different levels of responsibility under the DPA:

- “**data controller**” is the person who determines the purposes for which and the manner in which any personal data are, or are to be, processed;

² ICO Technical Guidance - Determining what is personal data

B. What is Data Protection?

- “**data processor**” is any person (other than an employee of the data controller) who processes personal data on behalf of the data controller.

If your organisation is a data controller, it is subject to all of the DPA’s requirements and responsible for deciding what data will be collected, its security, and how it will be processed. If your organisation is a data processor, e.g. an outsourced provider of payroll processing, then it has a more limited set of responsibilities under the DPA, including a responsibility to the individuals concerned for protecting the security of the personal data being processed.

B.2 The eight Data Protection Principles

The DPA establishes eight “Data Protection Principles” which set out the fundamental standards for dealing with personal information. They are as follows:

1. Data shall be processed fairly and lawfully.
2. Personal data shall be obtained and processed only for one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the DPA.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area without adequate protection.

B.3 Notifying the ICO

Data controllers must notify the ICO that they are processing information (unless they fall within limited exemptions). Even if they are exempt, they can still notify that they are processing data for exempt purposes to ensure that their business is seen as open and transparent. Notification involves the organisation’s details being added to a public register of data controllers and an annual registration fee (currently £35) is charged.

B.4 Enforcement by the ICO

The ICO may serve an information notice on companies, requiring them to provide specific information within a timeframe against which it can assess compliance with the DPA. The ICO does not have a general power to audit organisations’ processes without permission from the court. However, the government is currently consulting on awarding the ICO further inspection powers.

The ICO can issue an enforcement notice against an organisation once it becomes aware of a breach. The notice may require

B. What is Data Protection?

the organisation to take or not take specific steps to comply with the DPA. The ICO's most common action to date has been to require companies to give undertakings, as happened notably in March 2007 with 12 financial institutions.

The ICO cannot award compensation to individual data subjects if their personal data is misused, but a court can do so if direct financial loss can be shown.

Section 144 of the Criminal Justice and Immigration Act 2008 (which has received Royal Assent but is not yet in force) will give the ICO the power to fine companies for serious breaches of the DPA.

B.5 Criminal Offences

It is a criminal offence to fail to comply with information and enforcement notices issued by the ICO for which the fine is unlimited in a Crown Court (£5,000 in the High Court).

It is also a criminal offence to fail to notify (maximum penalty £5,000) and to knowingly or recklessly obtain, disclose or procure the disclosure of personal data without the consent of the data controller. The Criminal Justice and Immigration Act 2008 will extend this offence to carry a custodial sentence.

Section 61 of the DPA provides that if a company commits an offence with the consent or connivance of, or which is attributable to any neglect on the part of, any director, manager, secretary or similar officer, then that person is also guilty of that offence.

B.6 Other sources of data protection rules

Although the DPA is the key piece of legislation, there are a large number of other laws and regulations which will touch on the protection of personal information, such as the Freedom of Information Act 2000, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Environmental Information Regulations 2004 and the Human Rights Act 1998.

FSA-regulated firms are also required to "*establish and maintain effective systems and controls*" not only for compliance with legal and regulatory obligations but specifically to prevent and counter financial crime (see section A.2 above). In addition, rules exist to deal with specific types of personal information. For example, the Payment Card Industry Security Standards Council (PCI SSC) has established a common standard for the secure handling of payment card data.

C. Specific Data Protection Issues

C.1 Business issues

C.1.1 Direct marketing

Direct marketing to named individuals is affected by the DPA, as it enables individuals to request an organisation to stop using their personal data for direct marketing purposes.

In addition, the Privacy and Electronic Communications (EC Directive) Regulations 2003 apply to the sending of direct marketing messages by electronic means such as by telephone, fax, email, text message and picture (including video) message and by use of an automated calling system. They impose different restrictions on organisations depending on the method of marketing used. They also require an organisation to tell visitors to its website if a cookie or other tracking system collects information, and it must give them the opportunity to refuse their continued use.

Data sharing is common practice in some areas for marketing purposes but must be carried out carefully to avoid breaching the DPA. The ICO is considering the use of and regulation around data sharing and may update current guidance in the future.

C.1.2 International transfers of information

The DPA requires that where personal information is transferred to any country or territory outside the European Economic Area there should be an adequate level of protection in place.

The first step for the data controller will be to consider whether the other country's laws adequately protect personal information.

This generally means providing protection equivalent to that under EU law. The European Commission maintains a list of acceptable countries.

The USA is not considered to provide adequate protection by the European Commission. However transfers are permitted to US entities that adhere to the "Safe Harbor" scheme. This scheme has been approved by the European Commission. It allows individual US companies to register to certify that their data privacy standards will conform to a set of privacy principles, similar to EU standards. However, it is largely a self-certification scheme, and take up has been low.

If the country does not provide adequate protection, data controllers must ensure that the contract with the data processor contains detailed provisions dealing with this aspect. The ICO has approved the use of the European Commission's Standard Contractual Clauses for the transfer of personal data to either data controllers or data processors in third countries which can be used independently or incorporated into an outsourcing contract. However, this does not prevent a data controller from taking the view that other contractual terms would achieve the same result. The ICO has produced several guidance papers including *International transfers of personal data*.

C.1.3 Datarooms

Datarooms are widely used for corporate transactions such as the sale of a business. If any personal data will be transferred, parties should consider who is the data controller or data processor, if anyone will be accessing the dataroom from outside the EEA and whether providing anonymous data is a viable solution.

C. Specific Data Protection Issues

C.1.4 Subject Access Requests (SARs)

Data subjects have a right to know whether an organisation holds their personal data, i.e. they are entitled to see all the information which constitutes their personal data held by the data controller, and to have it corrected if it is incorrect or deleted if it is unnecessary. Organisations have only 40 days to provide information and there are only very limited situations in which they can refuse to do so, regardless of the applicant's motives, the scope of the SAR, and to some extent, the cost of compliance to the organisation. The ICO has published a *Checklist for handling requests for personal information (subject access requests)*.

To try to limit the amount of data that must be disclosed, organisations should ensure that staff think about what information they record and ensure their policies provide that data is not retained unnecessarily. Similarly, policies on the usage of CCTV and call recordings should take account of SARs.

Some special issues raised by SARs by employees are discussed in section C.2.5 below.

C.1.5 Monitoring business and employee activity

An organisation should carefully consider, and document, whether monitoring of phone and/or computer systems is necessary to protect a legitimate business activity before any action is taken. Measures adopted must be proportionate, balancing individual human rights (in particular, the right to privacy) against commercial advantages. Monitoring of staff should comply with the ICO's *Employment Practices Code*.

In addition, if a company needs to intercept electronic communications (for example, to record evidence of transactions, ensure regulatory compliance, detect crime or unauthorised use of the company's systems) it must comply with the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations³, which require users to be notified in advance that their activities may be monitored.

CCTV images obtained in a business context will be covered by the DPA and will need to be notified to the ICO, particularly those more advanced systems which, for example, can zoom in to monitor the activities of staff or individuals. The ICO's *CCTV Code of Practice* sets out guidance for users of CCTV and similar surveillance equipment.

C.2 Other Employee Issues

C.2.1 Proper handling of employee information

The DPA does not seek to prevent employers from carrying out acceptable collection and processing of data necessary to run their businesses properly. However, it strives to strike a balance between the legitimate needs of an employer and the need to protect the personal details of staff from abuse.

The ICO has published *The Employment Practices Code* and *The Employment Practice Code: Supplementary Guidance* for employers which cover such topics as recruitment, employment records, monitoring at work and information about workers' health.

³ SI 2000/2699 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

C. Specific Data Protection Issues

In particular, an organisation must be aware of its data protection obligations in:

- recruiting and selecting employees;
- dealing with employment records;
- collecting and processing sickness records and staff medical details;
- collecting information about staff to administer a pension or insurance scheme;
- collecting other sensitive information (e.g. about worker's disabilities, race or sexuality); and
- taking disciplinary action.

An organisation should, as a matter of good practice:

- use the information it collects on candidates for recruitment or selection only, and delete it once there is no further need to keep it;
- only ask for information about criminal convictions if this is justified by the type of job;
- make sure staff know how it will use records about them and when it will disclose the information. It does not need to get the consent of workers to keep legitimate records about them;
- delete information that it has no genuine business need for or legal duty to keep;
- let workers check their own records periodically. This will allow mistakes to be corrected and information to be kept up to date;

- keep employment records secure. Make sure that only staff with proper authorisation and the necessary training have access to employment records; and
- ensure it has in place proper procedures for collecting and handling sensitive data about staff (e.g. information on race, sex or disabilities).

C.2.2 The Transfer of Undertakings (Protection of Employment) Regulations (TUPE)

TUPE is a sensitive area for any business. Although a transferee employer may want as full a disclosure as possible, the right balance must also be struck in protecting transferee employees' data. The ICO has therefore published *Good Practice Note – Disclosure of employee information under TUPE*. This provides guidance on the apparent discrepancy between the obligation to disclose personal data in TUPE situations and the DPA obligations, and should be considered in any situation in which TUPE may apply. The interests of transferee and transferor employers, and transferring employees, can also be served by providing information in stages, e.g. by providing anonymised information if a TUPE liability is still being assessed, and personalised information once a TUPE liability has crystallised. This enables parties to ensure that the information disclosed is proportionate and necessary, bearing in mind obligations under both TUPE and the DPA.

C. Specific Data Protection Issues

C.2.3 Pre-employment practices

Before candidates are accepted for a new job, organisations often wish to obtain information from third parties about the new joiner. Organisations should be aware of the difference between verifying information provided by the candidate with third parties and ‘vetting’ candidates by gathering a wider range of new information to which they have not been granted access by the candidate. Any checks used should be proportionate and necessary to achieve the organisation’s needs.

As a general rule, intrusive checks should be delayed until shortlist or job offer stage, as should the need to obtain consent to process sensitive information. In some circumstances, criminal records checks may be required to be made with the Criminal Records Bureau (CRB). Checks cannot be carried out on all employees, and employers must comply with the Rehabilitation of Offenders Act 1974 and the CRB’s Code of Practice for recipients of disclosure data⁴. Records of criminal offences will be sensitive personal data for the purposes of the DPA, and retention and storage of the results of CRB checks should be limited and follow the specific guidelines set out by the ICO in the Employment Practices Code⁵.

C.2.4 Automated decision taking

Data subjects must be given additional information where their personal data is used for decisions that are automated, for example CV or initial job application scoring.

C.2.5 Employee SARs

Employees are entitled to know what personal data their employer maintains on them, and to have it corrected, in the same way as any other data subject (see section C.1.4 above). However, special issues may arise if (as is often the case) an employee serves the SAR in connection with an actual or potential dispute with the employer.

The employer may perceive the SAR as being designed to cause a nuisance by forcing it to trawl through emails and other electronic records – i.e. as a “fishing expedition” or “wild goose chase” at its own expense, or as a strategy to force it to disclose information earlier than it would have to under the Civil Procedure Rules.

The ICO does not accept that the fact that an applicant is contemplating or has already begun legal proceedings entitles a data controller to refuse to comply with an SAR. However, it notes that “*the courts do have discretion as to whether to grant an order under section 7(9) [of the DPA] and may be reluctant to exercise that discretion where it is clear that the purpose of the request is to fuel separate legal proceedings and, importantly, where the discovery rules under the Civil Procedure Rules would provide a more appropriate route to obtaining the information sought. The Commissioner is also likely to take such matters into account when considering whether to exercise his enforcement powers under section 40.*”⁶

The DPA does not include an express provision enabling an employer to refuse to comply with a SAR because compliance is too onerous or costly. However, the concept of proportionality does apply. The obligation to provide a copy of personal data

⁴ http://www.crb.org.uk/PDF/code_of_practice.pdf

⁵ <http://www.crb.gov.uk>

⁶ ICO Technical Guidance – Subject access requests and legal proceedings

C. Specific Data Protection Issues

under an SAR is tempered if the supply of a copy is not possible or would involve disproportionate effort. However, the employer will still be required to provide the employee with a description of the personal data held. Whether a request is disproportionate is measured against: the cost of providing the information; the length of time it may take to provide the information; how difficult it may be to provide the information; and the size of the organisation of which the request is made. This “disproportionate effort” defence was used successfully in the case of *Ezysias v The Welsh Ministers* to temper a very wide SAR and limit the data provided to a narrow search⁷.

Data which records an employer’s intentions in relation to any negotiations with the employee does not need to be disclosed if the disclosure would prejudice those negotiations. This would be the case where there is an actual or potential dispute with the employee. However, at a later date, when the matter has been settled, this information may be subject to disclosure.

If an organisation reasonably requires additional information to locate the information requested under the SAR and the organisation tells the person making the request what it needs, the organisation does not have to deal with the SAR until the information requested is provided.

C.2.6 Whistleblowing

There is an inevitable tension with the Public Interest Disclosure Act 1998 (“PIDA”) which provides protection to “whistleblowers”. PIDA encourages individuals engaged by an organisation to raise their concerns about a malpractice by

protecting them from dismissal and victimisation, provided that they have acted in good faith. A record of the whistleblowing disclosure may well identify an individual, who subsequently makes an SAR request. The issue is then whether a copy of the whistleblowing record identifying the person who made the disclosure and any others mentioned in the record should be provided under an SAR. The record can be withheld from the person filing the SAR unless: (i) the record can be fairly redacted to conceal the identity of the individuals other than the data subject making the request; or (ii) the person who made the disclosure and all others identified in the record consent to the disclosure of the record; or (iii) it is reasonable in all the circumstances to comply with the request.

C.3 Freedom of Information

The concept of free disclosure of information held by public bodies is closely linked to data protection. The Freedom of Information Act 2000 (FOIA) applies to most public authorities and companies which are wholly owned by public authorities. FOIA gives to individuals and organisations the right to request access to information. The public authority must tell the applicant whether it holds the information, and must normally supply it within 20 working days, in the format requested, unless an exemption applies. One such exemption is when individuals use FOIA to request information about themselves. FOIA should not be used for DPA requests. Accordingly in such circumstances, the individual must reapply under the DPA.

⁷ [2007] All ER (D) 65

D. Governance for Data Protection

D.1 Establishing a data management framework

Information protection is a governance responsibility and, as such, your organisation should have in place a formal system to monitor and control the collection and handling of personal information. This may include:

- Adopting a formal data protection policy: The DPA does not require organisations to have a data protection policy, but such a policy is certainly advisable for any large organisation. It may be a standalone document, or incorporated in a staff handbook.

The policy should state the types of personal information that the organisation collects, the reasons for collecting that information, the use it will make of that information, and who it may be disclosed or transferred to. It should notify the organisation's staff of the importance of data protection to the organisation, and how they can and should help the organisation to comply with its obligations under the DPA. The policy should also cover data security (see section D.3 below). It may provide for the appointment of a data protection officer (see section D.2 below) as the business process and policy owner for the business.

In addition, the organisation should set out its policy on routine monitoring that the organisation will perform and why it is necessary. It should inform staff of their right to submit a SAR and how they should do this. It may also require relevant staff to be given training on the policy and

any specific procedures that apply to them.

- Regular staff training: Staff should be familiar with the organisation's data protection policies and procedures (particularly those specific to their area), information security measures, how to deal with requests from individuals to access and correct information held about them and the consequences of non-compliance;
- Stakeholder departments adopting their own data protection procedures and processes: HR should have procedures for dealing with the personal details of job candidates and employees, including any sensitive personal data (such as sickness details), and they should receive targeted training on these procedures. IT will be responsible for security of the organisation's systems including the use of firewalls, passwords and the secure transfer and storage of personal information. These procedures and processes should consider:
 - how and why information is obtained and processed
 - how information is kept accurate, complete and up-to-date
 - how to delete and cleanse system records of information once no longer required for processing
 - appropriate controls on access to personal information held,

and the other matters referred to in sections D.2 and D.3 below.

- Adopting the necessary protections in contractual arrangements: If the organisation outsources to another organisation, it should have in place a

D. Governance for Data Protection

written contract which provides that the other organisation only uses and discloses any personal data in line with the outsourcing organisation's instructions and takes appropriate security measures to protect the data. Additional safeguards may be relevant where data is transferred outside of the EEA (see section C.1.2 above).

- Formulating and adopting a breach management plan: The plan would cover procedures for the containment of a breach and recovery of lost information, the assessment of ongoing risk, notification of the breach to the ICO (and other relevant authorities such as the FSA) and evaluation of the root cause.
- Auditing the collection and use of personal information: An audit of the personal information which the organisation collects, stores and processes should enable the organisation to establish whether its data protection policy and procedures are up-to-date and comprehensive, and the organisation's level of compliance with them. The ICO has issued a Data Protection Audit Manual which can be used to verify that there is a formal (i.e. documented and up-to-date) data protection system in place; that all the staff involved in data protection are aware of the existence of the data protection system, and understand and use the data protection system; and that the data protection system actually works and is effective.
- Conducting Privacy Impact Assessments (PIAs) for new systems: The ICO has issued a PIA Handbook which helps organisations to consider

data protection implications as part of any new initiative or change to ensure that mechanisms for complying with the DPA are integrated into new systems.

D.2 Monitoring data protection compliance

It is important that an organisation has a structure in place to monitor and report to management on its compliance with the data protection requirements. The DPA does not require organisations to appoint a data protection officer (DPO). However, given the importance of data protection to most organisations, it is advisable for their boards to allocate responsibility to a senior manager for ensuring that the organisation has a strong data management framework, and as a person to whom staff may go if they have any concerns about the way in which the organisation is managing and protecting the data which it holds on its staff and other individuals.

Depending on the nature and business of the organisation, the DPO could be the Head of HR, Legal or IT, or from a completely different area. Regardless, he or she will need to be sufficiently senior, credible and independent to command the respect of both staff and other senior management, and be given adequate authority and independence to carry out his or her duties. If you, as in-house lawyer, are asked to take on this role, you should ensure that you are capable of fulfilling it, and in particular that you have been given adequate authority and independence by the organisation (see section E.5 below).

It is important to understand that business policy and law may not always be aligned – for example there are advisory standards on

D. Governance for Data Protection

marketing mailing opt ins where the policy standard that the business wishes to operate may deviate from best practice guidance and/or the black letter law.

The DPO's role and responsibilities may include:

- providing or supervising training on the DPA, and the organisation's own data protection policy;
- monitoring the organisation's compliance with the DPA and its own data protection policy;
- auditing the organisation's collection and use of personal data, and performing PIAs;
- handling SARs (see sections C.1.4 and C.2.5 above) or reviewing how they are handled by others (e.g. HR and IT);
- investigating complaints and either resolving them or recommending to the board how they should be resolved;
- reporting to the board and/or senior management on data protection; and
- reporting any significant breaches of the DPA to the ICO and/or other regulators.

D.3 Data security

A key element of good data protection practice is the implementation of data security measures, including the use of "privacy-enhancing technologies". Under the Seventh Data Protection Principle, organisations are required to put in place both organisational and technical measures to ensure that data is protected. The aim is to prevent unauthorised accessing, alteration, or loss of personal information. The protection required for any specific data will need to be tailored for each situation so that it is proportionate and appropriate.

Consideration should be given to the sensitivity of the data and potential damage if it were lost or accessed and such sensitivity should be balanced against the cost of security.

Some practical steps may include:

- ensuring that the organisation's computer system has access controls preventing access to (or downloading of) personal data without the necessary authorisation;
- ensuring that any personal data downloaded to external devices (e.g. laptops, computer discs and pen drives) is encrypted; and
- ensuring that documents containing personal data which are due to be disposed of in accordance with the organisation's data retention policy are shredded or destroyed, not just thrown away.

ISO/IEC 27001 (dual numbered BS 7799-2:2005) is the international information security management systems standard. Organisations which meet the standard can obtain formal certification from the British Standards Institution (BSI). As the BSI points out, this may be particularly suitable where the protection of information is critical, such as in the finance, health, public and IT sectors, and for organisations which manage information on behalf of others, such as IT outsourcing companies, so that they can assure their customers that their information is being protected⁸. Other organisations can perform an internal self-assessment against the standard, and can use the standard to help them formulate an information security policy and procedures.

⁸ See www.bsigroup.co.uk/en/Assessment-and-Certification-services/Management-systems/Standards-and-Schemes/ISOIEC-27001/

D. Governance for Data Protection

The FSA's Financial Crime & Intelligence Division has recently published a major report on data security in financial services⁹. The report looks at how regulated firms are addressing the risk that their customer data may be lost or stolen and then used to commit fraud or other financial crime. The report concludes that "... *poor data security is currently a serious, widespread and high-impact risk to our objective to reduce financial crime*". It warns that many firms, particularly small ones, need to make substantial progress to protect their customers from the risk of identity fraud and other financial crime. The FSA's report sets out detailed guidelines establishing good data security practice for regulated firms on governance, training and awareness for staff and staff recruitment and vetting, as well as the way firms should control:

- access rights
- passwords and user accounts
- access to customer data
- data back-up
- access to the internet and email
- key-logging devices
- laptops
- portable media including USB devices and CDs
- physical security
- disposal of customer data, and
- processing of data by third-party suppliers.

Organisations which are regulated by the FSA should, if they have not already done so, review their data security to ensure that they comply with these guidelines.

⁹ *Data Security in Financial Services – Firms' controls to prevent data loss by their employees and third-party suppliers* (April 2008)

E. Future Directions

E.1 Data Sharing Review Report

In July 2008, Richard Thomas, the Information Commissioner, and Dr. Mark Walport of the Wellcome Trust presented their report on data sharing to the Prime Minister¹⁰. Whilst the focus of the report was data sharing primarily between Government departments, it also looked at general aspects of data protection good practice.

Mr. Thomas and Dr. Walport concluded that “*The case for change is strong. The law and its framework lack clarity, responsiveness and bite. Public confidence is evaporating and technology continues to advance. While there can be no quick or easy solutions, a package of clearly targeted measures could radically transform the way personal information is collected, used and shared.*”. They then made wide-ranging recommendations which signpost the authors’ preference for more stringent standards of data protection governance and practice, including:

Recommendation 1: *As a matter of good practice, all organisations handling or sharing significant amounts of personal information should clarify in their corporate governance arrangements where ownership and accountability lie for the handling of personal information. This should normally be at senior executive level, giving a designated individual explicit responsibility for ensuring that the organisation handles personal information in a way that meets all legal and good-practice requirements. Audit committees should monitor the arrangements and their operation in practice.*

Recommendation 2: *As a matter of best practice, companies should review at least annually their systems of internal controls over using and*

sharing personal information; and they should report to shareholders that they have done so.

Recommendation 3: *That organisations take the following good-practice steps to increase transparency:*

(a) *Fair Processing Notices should be much more prominent in organisations’ literature, both printed and online, and be written in plain English. The term ‘Fair Processing Notice’ is itself obscure and unhelpful, and we recommend that it is changed to ‘Privacy Policy’.*

(b) *Privacy Policies should state what personal information organisations hold, why they hold it, how they use it, who can access it, with whom they share it, and for how long they retain it.*

.....

Recommendation 9: *That the Information Commissioner’s investigation and audit powers be extended and that sanctions should mirror the existing sanctions available to the Financial Services Authority, setting high, but proportionate, maxima related to turnover.*

E.2 The Information Commissioner’s views on governance

The Information Commissioner summarised his views in a recent speech¹¹:

“All of this must ultimately be a matter of good governance and accountability. There is no single magic bullet, but there will always be three key elements:

¹⁰ www.justice.gov.uk/docs/data-sharing-review.pdf

¹¹ Speech to RSA Conference Europe on data breaches – Richard Thomas, Information Commissioner – 29 October 2008

E. Future Directions

- *Clear thinking and paperwork – Ensuring the right policies, procedures, contracts, compliance arrangements etc.*
- *Getting the technology right – Awareness of the power of technology, the risks of ever-cheaper storage and mobile data and looking to use technology to minimise risks - “Privacy by Design”.*
- *Focussing on people and behaviour – Recognising that the challenge is cultural and psychological - and must be led from the top – with the right approaches to awareness programmes training, managements, and supervision.*

Those at the top of organisations – chief executives, permanent secretaries and so on – must be certain that the right framework is in place to address the risks of personal information and must be certain that responsibilities are clear. There must be complete clarity on who, inside each organisation, has responsibility for safeguarding each set of personal data. This is equally important where data is shared, sometimes amongst several sources, and where processing is outsourced to contractors. Given the levels of risk, there is also a role here – as we elaborated in the Thomas-Walport Report on Data Sharing – for reassurance to be provided through Audit Committees and Statements of Internal Control in annual reports. This should be enlightened self-interest and bodies such as the CBI can help to ensure adequate controls and disclosures. But the Financial Reporting Council and others will need to intervene if high-level accountability is not achieved in practice.”

E.3 Ministry of Justice Response to the Data Sharing Review Report

The Ministry of Justice (MoJ) responded to the Data Sharing Review Report in

November 2008¹². It agreed with many of the recommendations of the Review Report which appear to have wider data protection implications than data sharing. Echoing the Review Report, the MoJ stated that “Measures need to be taken to increase public trust and confidence in the handling and processing of personal data by both the public and private sectors.”

The MoJ noted that it was already working with the ICO to determine the level at which maximum penalties should be set for serious breaches of existing data protection legislation.

There is therefore a clear determination on behalf of the Government to recognise the concerns raised by the Information Commissioner, as soon as the Parliamentary timetable permits (given the more urgent need to implement measures to rescue the economy). This may result in wider powers and penalties in the ICO’s armoury. These are likely to be coupled with more detailed rules on how organisations should structure and manage data protection governance, with more emphasis on the personal involvement of senior management.

E.4 New BSI standard

The BSI is developing a new data protection standard for the management of personal information. Intended for publication in June 2009, the standard aims to help organisations put in place an infrastructure for effective compliance¹³.

¹² Ministry of Justice, Response to the Data Sharing Review Report, 24 November 2008, available at <http://www.justice.gov.uk/publications/response-data-sharing-review.htm>

¹³ Draft BS 10012 *Specification for the management of personal information in compliance with the Data Protection Act 1998* available at <http://www.bsi-global.com>

F. The In-House Lawyer's Role in Data Protection

F.1 Difficulty of defining the role of the in-house lawyer

Virtually all organisations in the UK have data protection obligations arising from their collection and maintenance of personal data about staff, customers, stakeholders, pension holders and others. However, the role of the in-house lawyer will vary depending on the size and business of the organisation, its management, IT and legal structure and group (or key supplier/customer) presence in other jurisdictions where the standards that need to be addressed may vary significantly. Nevertheless, some broad principles can be helpful to give some guidance on the role of the in-house lawyer¹⁴.

F.2 Management ownership

The importance of management buy-in and ownership of this all-pervasive issue cannot be overestimated. Whether or not the organisation has data protection policies, or has appointed a DPO, it must not lose sight of the fact that the board and senior management ultimately retain responsibility and must be proactive in instilling and maintaining a data protection culture within the organisation.

The in-house lawyer can assist the board and senior management to understand the importance of data protection and their responsibilities and exposures (both functional and personal) under the DPA and under other applicable regulatory regimes, such as the FSA rules or quasi regulatory

regimes such as the PCI SSC rules. They can provide detailed training, or could arrange for some other suitably skilled person to do so. They will need to frame their advice in a way that understands and takes account of the functional needs, requirements, priorities and resources of other functions in the business (such as the HR and IT functions) to ensure that their advice is usable and therefore worked with rather than ignored or misapplied.

The in-house lawyer can assist the board to formulate and adopt a data protection policy (see section D.1 above), consulting the relevant functions and drawing on the findings of any recent data protection audits and PIAs. The in-house lawyer and the DPO roles should be clearly distinguished – especially if the same person is carrying out both roles, so as to ensure that the difference between legal advice and internal policy is clearly understood.

F.3 Managing enforceability risks

It is important to ensure not just that the business has framed a policy with a clear understanding of legal requirements, but also that its contractual paperwork is compliant with legal requirements and that the business understands what will need to be done with that paperwork to maintain this. For example, having an outsourcing contract that is right on paper but not adhered to in practice is pointless; substance is as critical as form in this area. In many organisations the roles of advisor, organiser and compliance enforcer on data privacy areas can become blurred – especially in respect of issues that are identified by the in-house lawyer not to be operating correctly, because the in-house lawyer has come across

¹⁴ See also *A Fine Line*, the second set of Guidelines published by the Corporate Governance Committee in July 2006, available at <http://www.cigroup.org.uk/cgpub.aspx>

F. The In-House Lawyer's Role in Data Protection

the problem in the ordinary course of their work. We have given guidance in *The Fine Line* on the importance of making these roles clear in policy and in practice to ensure that the in-house lawyer can operate effectively.

F.4 Managing regulatory risks

Regulatory risks come from both conscious policy decisions that the business has to take in response to conflicting resource, prioritisation and budget requirements and ambiguities in the legal position. The in-house lawyer has an important role to play both in helping the business to take an informed decision as to risk and in helping to keep the board and management focused on reviewing that risk level regularly in the light of changes in the legal, regulatory and guidance framework and in the light of changes in business practices, systems etc. The ICO is enforcing its own policies more actively and vigorously. Standards that may have been acceptable two years ago may not be now or in the future. The in-house lawyer can also play an important role in advising the DPO on how to manage communications with regulators and on third party (customer, employee, etc) complaints and litigation.

F.5 Should the in-house lawyer be the DPO?

As mentioned in section D.2 above, it is advisable for boards to allocate responsibility to a senior manager for ensuring that the organisation has a strong data management framework, and as a person to whom staff may go if they have any concerns about the way in which the

organisation is managing and protecting personal data.

The DPO role is an important one, and it requires skills, training and experience as well as a substantial commitment in terms of available time. Two of the most challenging aspects of the role are likely to be:

- dealing with other functions such as HR and IT, as they may be sensitive to scrutiny on how they handle and protect staff data and/or respond to employee SARs; and
- mastering the information security aspects of maintaining, protecting and retrieving personal data held by the organisation.

If you are asked to take on this role, you should ensure that you are capable of fulfilling it, and in particular that the organisation has given you adequate independence, authority, resources and access to information and personnel, to perform the role to a high standard¹⁵.

You should also ensure that you can continue to perform your “day job” as in-house lawyer to a high standard.

You should perform the role fairly, impartially and discreetly, with reference to the organisation’s data protection policy (if

¹⁵ Note that the Thomas/Walport Data Sharing Review Report recommends that organisations which handle or share significant amounts of personal information should designate a specific individual who has ownership and accountability lie for the handling of personal information, and that this person should normally be at senior executive level (also see section E.1)

F. The In-House Lawyer's Role in Data Protection

any). You should keep good notes of your decisions, investigations and recommendations, as your actions may well be scrutinised if there is litigation or publicity later. Remember that your notes and communications (in this capacity) are likely to be disclosable, except when you are yourself obtaining legal advice. Try to avoid any conflicts of interest with your other functions and, if you find that you have any, ensure that you declare them promptly to the senior management and/or the board.

Your independence and authority could be severely tested if an employee delivers a SAR and the organisation's management wish to resist responding to it on the grounds that it is too broad, or is connected with a grievance or actual litigation (see section C.2.5 above), or if the senior management want to conduct some non-routine monitoring of a particular employee because that employee has a grievance against the organisation. If you have taken on the role of DPO, you will have to give your advice impartially, and in a particularly difficult situation you may need to obtain independent external advice.

Ensure that staff are aware that your duties are to the organisation, and that you cannot give them any legal advice individually, and cannot guarantee them confidentiality within the organisation, if they complain to you about a possible breach by the organisation or another member of staff of the DPA or the data protection policy.

F.6 Handling significant breaches

Whether or not you are nominated as the DPO, if you observe any significant breaches by the organisation of the DPA or

any related laws and regulations, you should ensure that these are reported to the ICO and any other relevant regulator such as the FSA. Serious breaches must not be covered up and the in-house lawyer has an important role to play in assisting the organisation to face up to its responsibilities, cooperate with the relevant authorities and ensure that corrective action is taken.

Where there is reluctance or outright opposition, we refer you to the advice we gave in *A Fine Line*, namely that you should appeal to the independent non-executive directors (if your organisation has any) and, if that fails, in extreme circumstances you may have to threaten to – or actually – “blow the whistle” internally and/or externally, and/or resign¹⁶. These issues are discussed in more detail in *Blowing the Whistle*¹⁷.

F.7 Keeping pace

In-house lawyers have an important role to play in helping their organisations establish and maintain a robust data management framework, but to do so they must keep pace with the risks posed by rapidly developing technology, as well as developments in risk management and corporate governance practice and regulation. If they fail to do so, they risk being sidelined in this very important area, and their organisations may suffer as a result.

¹⁶ *A Fine Line*, Section E.8

¹⁷ *Blowing the Whistle*, the third set of Guidelines published by the Corporate Governance Committee in April 2007, available at <http://www.cigroup.org.uk/cgpub.aspx>. See Section E

Acknowledgements and disclaimer

The information contained in this document is given in good faith with the intention of furthering the understanding of its subject matter. Whilst the Corporate Governance Committee of the Commerce & Industry Group (“Committee”) believes that it is accurate and up-to-date as at the date on which it was approved for publication (20 January 2009), none of the Committee, the Commerce & Industry Group, the Law Society of England and Wales, or any of their respective members or employees accept any liability:

- For any loss or damage occasioned by any person or organisation acting or refraining from taking action as a result of any view expressed in this document. If readers have concerns about the subject matter, they are advised to seek independent advice based on the circumstances of their own situation; or
- In respect of the availability or content of any third party site or publication referenced in this document.

The views and opinions expressed in this document are not necessarily to be attributed to the organisations represented by Committee members.

The C&I Group Corporate Governance Committee would like to thank Patrick Brodie of Wragge & Co LLP for his comments on earlier drafts of these guidelines. The Committee of course retains responsibility for the final version.

The Commerce & Industry Group is a recognised Law Society Group run by in-house solicitors – who give their time freely – to provide services to its members.

The C&I Group has established a dedicated Committee to deal with a range of corporate governance issues, and is committed to addressing them in order to support its membership community.

For more information visit http://www.cigroup.org.uk/Regions_corp.gov.asp

© 2009 Commerce & Industry Group.
All rights reserved.