# Fully compliant? A study of data protection policy in UK public organisations

## Volume 1

by

**Adam Warren**

A Doctoral Thesis

submitted in partial fulfilment
of the requirements for the award of the degree of

Doctor of Philosophy
of
Loughborough University

June 2003

Department of Information Science

Student Office, Academic Registry
Loughborough University Loughborough Leicestershire LE11 3TU UK
Switchboard: +44 (0)1509 263171 Fax: +44 (0)1509 223905

Loughborough University

## CERTIFICATE OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this thesis, that the original work is my own except as specified in acknowledgments or in footnotes, and that neither the thesis nor the original work contained therein has been submitted to this or any other institution for a higher degree.

( Signed )

3/3/03

( Date )

# Fully compliant? A study of data protection policy in UK public organisations

## Abstract

The aim of this thesis was to investigate and analyse the extent to which public organisations have achieved compliance with the Data Protection Act (DPA) 1998. In order to achieve this aim, two hypotheses were tested. The primary hypothesis assessed whether the DPA 1998 represented a positive measure for ensuring compliance and good practice in public organisations. The secondary hypothesis considered the extent to which the DPA 1998 strengthened individual informational privacy, setting the Act in context with previous data protection legislation – in the UK and abroad. Moreover, the provisions of the DPA 1998 were critically compared with other key UK statutes, including the Human Rights Act 1998 and the Freedom of Information Act 2000.

The two hypotheses were tested through triangulation of research. Desk research analysed literature in this field and the legal origins of the DPA 1998. Key issues impacting on data protection were identified and the challenges of recent UK legislation outlined. Consideration was given to challenges posed to organisations when handling data belonging to their employees. The findings were supported by fieldwork interviews with experts in policy-making, law and campaigning. A questionnaire survey was distributed to nearly 400 organisations in order to gain indicative data regarding compliance. This provided a gateway for case study interviews with Data Protection Officers (DPOs) from 18 public organisations.

The thesis concluded that the majority of participants had implemented considerable changes in corporate practices in response to the provisions of the DPA 1998. Important measures included: increased status and influence of the DPO; development of detailed staff training plans; implementation of procedures facilitating the efficient handling of data subject access requests; and approval of detailed data protection policies and procedures designed to ensure compliance permeated the organisation. Finally, recommendations have been made for improved best practice, including the creation of an integrated records management post, and enhanced information security.

# Fully compliant? A study of data protection policy in UK public organisations

## Volume 1

## Contents


Acknowledgements vii

Abbreviations viii

**1. Introduction** **1**

**1.1 Introduction** 1

1.2 Aim 4

1.3 Hypotheses and key objectives 4

1.4 Outcomes 8

**2. Methodology** **11**

**2.1 Introduction** 11

2.1.1 Research methodology texts

2.1.2 Developing a methodology

2.1.3 Triangulation of research

**2.2 Desk research** 20

2.2.1 Documentary analysis

2.2.2 Literature review

2.2.3 Current legal situation

2.2.4 Other research in the field

**2.3 Fieldwork** 23

2.3.1 Questionnaire survey

*Purpose and design*

*Pilot questionnaire*

*Amendments following pilot questionnaire*

*The full questionnaire survey*

*Distribution and return of questionnaires*

2.3.2 Expert interviews

2.3.3 Case studies

**2.4 Limitations of this study** 37

**2.5 Conclusions** 39

**3. Literature Review** 45

**3.1 Data Protection** 46

3.1.1 Landmark studies: the 'privacy' debate

3.1.2 Comparative research

3.1.3 Recent academic research 1995-2003

3.1.4 Sources of information on data protection

*Standard legal texts*

*Academic journals*

*Newsletters*

3.1.5 The wider debate

*Government*

*Non Government Organisations (NGOs)*

*Expert forums*

*Consumer opinion*

*Media debate*

**3.2 Human Rights** 62

3.2.1 Incorporation of European Convention of Human Rights

3.2.2 Privacy and human rights context

3.2.3 HRA 1998: recent research

*Analysis of case law 2000-2003*

**3.3 Individual privacy protection: the organisational dimension** 66

3.3.1 New legislative framework: potential for conflict?

3.3.2 Academic and legal research

3.3.3 Regulating employee personal data

**3.4 Conclusions** 70

**4. Data Protection and the Law** **85**

**4.1 Introduction** 85

4.1.1 Method

4.1.2 Objectives

4.1.3 Definitions: 'privacy' and 'data protection'

**4.2 The international scene: from guidance to legal enforcement** 89
**1967-1981**

4.2.1 The Nordic Conference

4.2.2 The Council of Europe

*Early Resolutions*

*Convention 108*

4.2.3 The Organisation for Economic Cooperation and Development (OECD)

*The OECD guidelines*

**4.3 'Top down': the role of the European Commission 1985-2003** 98

4.3.1 Context: The European Economic Community (EEC)

4.3.2 The case for a general Directive

*Different national approaches*

*The European single market*

*The Schengen Agreement*

*From Community to Union: structural reforms*

4.3.3 Data Protection Directive 95/46/EC: key provisions

4.3.4 Telecommunications Data Protection Directive 97/66/EC

*Electronic Communications (E-Communications) Directive 2002/58/EC*

**4.4 Europe: divergence to convergence** 110

4.4.1 Hesse: the first data protection law

4.4.2 Sweden: the first national data protection law

*Revision following Directive 95/46/EC*

4.4.3 Germany: federal data protection

*The Census Decision*

*Revision following Directive 95/46/EC*

4.4.4 The Netherlands: codes of conduct

*Personal Data Protection Act 2000*

**4.5 Data Protection in UK: context** 125

4.5.1 Common Law and the Younger Report on Privacy 1972

4.5.2 White Paper: *Computers and Privacy* 1975

4.5.3 The Lindop Report on Data Protection 1978

4.5.4 The UK Data Protection Act 1984

*Processes*

*Provisions*

*Development of data protection law*

**4.6 UK: DPA 1998** 138

4.6.1 Implementing a data protection infrastructure

4.6.2 Key provisions affecting information privacy

4.6.3 Key provisions affecting employees

*Codes of practice*

**4.7 North America** 145

4.7.1 United States

*The Constitution versus common law*

*Freedom of Information Act 1966*

*Privacy Act 1974*

*A 'Safe Harbor'?*

*Provisions*

*Enforcement*

*Reaction*

4.7.2 Canada

*The Privacy Act 1982*

*The Personal Information Protection and Electronic Documents Act 2000*

**4.8 Conclusions** 163

## Figure

1. Triangulation of research 18

## Tables

1. Examples of employee and client personal data 2

2. Distribution of questionnaires by category 30

3. Early ratification of Convention 108 by Council of Europe member states 1982-1990 93

4. Accession of member states to the European Community 98

5. European national data protection legislation prior to EU Data Protection Directive 1995 111

# Acknowledgements

Above all, I would like to thank Jo, for her considerable patience and understanding during the two and half years I have been absorbed by this thesis. Further acknowledgements go to my supervisors, Dr James Dearnley and Professor Charles Oppenheim for the support and expertise provided in contrasting, but equally significant, ways. Moreover, the academic librarians at Loughborough University's Pilkington Library proved particularly helpful during the first year of my research, complementing their knowledge of relevant texts and databases with a thoroughly professional service.

Naturally, this research would not have been possible without contributions from: various experts in policy-making, law and campaigning; respondents to the questionnaire survey; and, crucially, the Data Protection Officers from the eighteen public organisations that comprised the case studies for this project. Finally, special thanks goes to Sir Norman Lindop, chairman of the Data Protection Committee 1976-1978, for being a perfect host during a visit to his home in September 2001, and contributors to the online JISCmail data protection discussion list, for promptly answering the author's nagging queries.

# Abbreviations

*All legislation and organisations United Kingdom unless otherwise stated.*

| | |
|---|---|
| ACPO | Association of Chief Police Officers |
| ATCSA | Anti-Terrorism, Crime and Security Act 2001 |
| BSI | British Standards Institution |
| CBI | Confederation of British Industry |
| CCTV | Closed Circuit Television |
| CFOI | Campaign for Freedom of Information |
| CRB | Criminal Records Bureau |
| DIB | Data Inspection Board, Sweden |
| DOC | Department of Commerce, United States |
| DPA | Data Protection Act 1998 |
| DPO | Data Protection Officer |
| DTI | Department of Trade and Industry |
| ECHR | European Convention on Human Rights |
| EEA | European Economic Area |
| EHRR | European Human Rights Reports |
| EPIC | Electronic Privacy Information Center, United States |
| EU | European Union, formerly the European Economic Community (EEC) |
| FOIA | Freedom of Information Act 2000 |
| FTC | Federal Trade Commission, United States |
| HRA | Human Rights Act 1998 |
| ICJ | International Commission of Jurists |

| | |
|---|---|
| ICT | Information and Communications Technologies |
| IDeA | Improvement and Development Agency |
| ILO | International Labour Organisation |
| IM&T | Information Management and Technology |
| ISDN | Integrated Services Digital Networks |
| ISEB | Information Systems Examination Board |
| ISP | Internet Service Providers |
| JILT | Journal of Information, Law and Technology |
| JISC | Joint Information Systems Committee |
| LBPR | Lawful Business Practice Regulations 2000 |
| LISU | Loughborough University's Library and Information Statistics Unit |
| MSF | Manufacturing, Science and Finance Union |
| NADPO | National Association of Data Protection Officers |
| NCC | National Computing Centre |
| NGOs | non-Governmental Organisations |
| NHS | National Health Service |
| Oe-E | Office of the e-Envoy, Cabinet Office |
| OECD | Organisation for Economic Cooperation and Development |
| OIC | Office of the Information Commissioner, formerly the Office of the Data Protection Registrar (ODPR) |
| OMB | Office of Management and Budget, United Sates |
| PDA | Personal Data Act 1998, Sweden |
| PIPEDA | Personal Information Protection and Electronic Documents Act 2000, Canada |
| PPSC | Privacy Protection Study Commission, United Sates |
| RIPA | Regulation of Investigatory Powers Act 2000 |

| | |
|---|---|
| SARs | Subject Access Requests |
| SIS | Schengen Information System |
| SOCITM | Society of Information Technology Management |
| TUC | Trades Union Congress |
| UNICE | Union of Industrial and Employers' Confederations of Europe |

# 1. Introduction

## 1.1 Introduction

The concepts of data protection and individual privacy are fraught with difficulties, raising questions from the outset. Firstly, what constitutes data protection? Is it a human right founded on the desire to preserve personal privacy, or merely a set of strict legal conditions relating to the quality and nature of data? In this thesis, the term 'data protection' (also known as 'information privacy') is used to describe the individual's control over the circulation of their personal information[1].

Secondly, how do data protection considerations fit into organisational processes for information handling? This is a vast and complex area, with organisations – and their needs for personal data – taking many forms. Out of necessity, this study had to draw boundaries, and the scope of the thesis is limited to researching the information handling processes of public organisations. Whilst acknowledging that boundaries between public and private sectors are becoming increasingly blurred, significant recent legislation has been enacted in the UK applying specifically to the public arena. In particular, public authorities will by 2005 have to comply with the provisions of the Freedom of Information Act (FOIA) 2000. The relationship between FOIA 2000 and the Data Protection Act (DPA) 1998, especially amendments the former makes to the latter, will be discussed in detail in Chapter 5 (section 5.4). In addition, since October 2000, public authorities have been directly affected by the Human Rights Act (HRA) 2000, incorporating the European Convention of Human Rights (ECHR) into UK law. Again, this is discussed in Chapter 5 (section 5.3), with particular reference to the ECHR Article 8 - right to a private life. Appreciation of the relationship between the DPA 1998 and the above (and other) related statutes, is important in assessing the extent to which public organisations can achieve data protection compliance.

Furthermore, at a micro-level, it is difficult to consider how organisations handle personal data without investigating the protection of data belonging to their

employees, as well as data collected from the general public (or 'clients') during the performance of their corporate duties. Examples of data from both categories are given below:

| *Personal data acquired about employees.* | *Personal data acquired during performance of corporate duties.* |
|---|---|
| Include: references received, sickness records, next of kin details, annual appraisals, accident/injury at work and pension contributions. Much of the above data are collected due to statutory obligations. | Dependent on the nature of public authority, examples include: council tax details, medical records, criminal convictions, data captured by Closed Circuit Television (CCTV) and education records. |

Table 1: Examples of employee and client personal data

Whilst in theory all personal data has to be processed in line with the eight principles outlined in DPA 1998[2], the handling of data belonging to employees poses particular challenges. For example, the issue of employee 'consent' for the processing of sensitive data, and how this can be freely given in what is generally considered to be an unequal relationship. Moreover, access to and processing of medical data can require particular attention in the employment context – with some employers needing to check whether an employee may be exposed to a health risk at work. In such circumstances, the information should be kept to a minimum required for an employer to meet his obligations, and access restricted to the occupational health physician. Such issues have led to the drafting of an *Employment Practices Code of Practice*[3] by the UK national supervisory authority – the Office of the Information Commissioner (OIC) – and to the European Commission proposing further legislation in this field[4]. Therefore, whilst the overarching aim of this thesis considered organisational compliance with the DPA 1998 in general, this study would have been deficient if regulatory activity in the field of employee personal data, and the responses of public authorities, had been ignored.

Consequently, the processing of employee personal data featured prominently in various stages of research. Most notably, a questionnaire survey (refer to Appendix D) probed organisational handling of employee records, in addition to measuring general levels of awareness and informed opinion concerning data protection and related legislation. Additionally, employee data formed the focus of certain expert interviews with trade unionists and employers' organisations[5]. Finally, this issue was raised in general discussion with case study interviewees, chiefly in relation to handling of subject access requests (SARs)[6].

An example of the overlap between organisational and employee concerns was the case of the health authority, discussed in Chapter 7. In this organisation, two types of personal patient data were being held: data belonging to patients generally, and data belonging to patients who were also employees. Reconciling the privacy of the latter records with the legitimate needs of employees to access patient data proved problematic, and abuses of the system had occurred. Such dilemmas were present in all organisations handling personal information, although the nature of the personal data stored by health and police authorities in particular made these concerns more pressing. Yet, the questionnaire survey demonstrated that far fewer bodies had defined subject access procedures for employees *per se* than for tackling requests from the general public[7]. These findings were supported to a degree during interviews with case study organisations[8]. On the whole, organisations preferred to allow employees access to their personnel records on an informal basis, rather than through the submission of a formal SAR. Indeed, such an eventuality was considered to represent a "failure" in organisational procedures, and thus to be avoided[9].

Finally, the level of importance afforded to data protection issues by public organisations has been considered in this thesis. How much of a priority is data protection compliance when the rhetoric from central government encourages data-matching, 'joined-up government' and commercial access to public sector information – initiatives that potentially impact on information privacy?

It is the above, intertwined strands that will be investigated in this project, with case studies in particular highlighting the challenges public organisations, and in particular nominated individuals within those organisations, face in achieving data protection compliance in relation to both client and employee records.

## 1.2 Aim

The overall aim of the thesis is:

> **To investigate and analyse the extent to which public organisations have achieved compliance with the Data Protection Act (DPA) 1998.**

## 1.3 Hypotheses and key objectives

In order to achieve this aim, two hypotheses were tested. Hypotheses were chosen as they represent a preconception of what might true, against which various tests can be applied. They constituted a guide – continually referred to by the author during the progression of the research project. Moreover, the hypotheses served as statements about the relationships between variables (for example: the impact of various legal texts; the conduct of the supervisory authority in enforcing the DPA 1998; and the information handling practices of different organisations). Key objectives set out how each hypothesis was to be investigated.

**Hypothesis 1: At an organisational level, the DPA 1998 represents a positive measure for ensuring compliance and good practice.**

*Key Objectives*

- To survey attitudes of organisations towards the workability the DPA 1998 and other relevant legislation;
- To identify the actual processes involved in achieving compliance with the DPA 1998;
- To devise recommendations for best practice concerning data processing in organisations.

This primary hypothesis directly addressed the aim of the thesis, and was tested principally through a questionnaire survey and case study interviews with data protection practitioners[10]. Questionnaires were posted to a sample of public organisations to assess the impact of recent data protection and related legislation – such as the Human Rights Act 1998 - on individual informational privacy. Moreover, the survey charted the measures organisations have taken in order to ensure compliance. Finally, for the reasons outlined in section 1.1, the questionnaire focused on the processing of employee personal data. This investigation was followed up by in-depth, case study interviews with data protection officers from 18 of those organisations. The case studies aimed to: gauge reactions to the DPA 1998; assess the Act's workability; highlight any difficulties encountered; and define major changes to organisational practice brought about by the Act's implementation. The vast majority of interviewees were open, courteous, and generous with their time. Many had gathered documents of interest in advance, and others invited guests to the interview. Due to promised confidentiality, case study respondents have not been named in this thesis.

**Hypothesis 2: The DPA 1998 has built on previous legislation in the UK, and abroad, in order to strengthen the individual right to informational privacy. Within the UK, a regulatory framework has been established, enabling this right to be exercised effectively.**

- **The DPA 1998 works effectively with other legislation impacting on data protection. Overlap is minimal and meaning is clear.**

*Key Objectives*

- To set the DPA 1998 in context with previous data protection legislation – both in the UK and abroad;
- To critically compare and review academic studies on the effectiveness of data protection legislation, giving particular attention to policy recommendations;
- To identify the main provisions of the DPA 1998 concerning individual informational privacy;
- To identify measures taken UK supervisory authority, the OIC, to encourage data protection compliance;
- To critically compare provisions of the DPA 1998 and other key UK legislation, drawing out any ambiguities and potential for confusion.

This second hypothesis was deliberately wide-ranging. It sought to define the context to, and the recent development of, UK data protection law. Knowledge of legal and policy context was vital in order to draw conclusions about organisational compliance with the DPA 1998. Additionally, it was crucial to gain an understanding of the regulatory framework, in particular the extent to which it enabled compliance with the DPA 1998. Therefore, consideration has been given to the role of the OIC, particularly in promoting codes of practice, and to practitioner views on compliance advice received from the supervisory authority.

This hypothesis was divided into two parts. The overarching intention was to test how effectively the DPA 1998 strengthened the individual right to informational privacy. However, an important test of the privacy implications of the DPA 1998

lay in assessing how effectively the Act worked with other legislation impacting on privacy of personal information. The key legislation referred to in the subsidiary hypothesis, besides the DPA 1998, were:

- HRA 1998 – incorporating a European Convention on Human Rights into UK law;
- FOIA 2000 – providing a right of access to information held by public organisations. The Scottish Parliament passed a separate FOIA[11] in April 2002. This distinct legislation will apply to public authorities within the competence of the Scottish Parliament (for example, Scottish educational establishments and Scottish National Health Service trusts[12]);
- Regulation of Investigatory Powers Act (RIPA) 2000 - in part permitting the interception of electronic communications such as email.

In addition, consideration has been given to the implications of recent anti-terrorism legislation in the wake of the terrorist attacks in the United States on 11th September 2001[13].

Testing this hypothesis required considerable desk research. The literature in this field is extensive, including monographs and academic articles, standard legal texts aimed at lawyers, newsletters, newspaper articles and consumer surveys. The academic debate has been shaped by such monographs such as Westin's *Privacy and freedom*[14] and Rule's *Private lives and public surveillance*[15], and subsequently developed through the work of scholars such as Flaherty, Bennett and Raab[16]. At a practitioner level, newsletters and discussion lists have kept data protection officers in organisations informed of new developments in this evolving discipline.

The desk research was correlated by semi-structured expert interviews with individuals active in policy-making, law or campaigning. Examples of those interviewed include: government (such as the Lord Chancellor's Department and the Office of the e-Envoy); non-governmental organisations (such as JUSTICE and Consumers International); business interests; trade unions; the supervisory authority for data protection in the UK (the OIC); the European Commission in

Brussels; and various lawyers and legal advisors to government committees working in this field[17]. These interviews gave an insight into the diverse views on this topic, most notably concerning implementation and enforcement of the DPA 1998, and interaction with other key legislation such as the HRA 1998, RIPA 2000 and FOIA 2000.

## 1.4 Outcomes

The conclusions to this study draw together the main themes that emerged from the desk research and fieldwork. The goal has been to provide a critique of data protection compliance in public organisations. Recommendations have been produced, comprising:

- An evaluation of what has been researched in the case studies;
- Guidance as to how policy can further be developed.

The recommendations have been referred back to interested case study interviewees for comment, and the final version adjusted in light of their views. The intention throughout is to provide constructive criticism and to assess whether, over the 35 years following the publication of Westin's study, individuals are now in a position to 'determine for themselves when, how, and to what extent information about them is communicated to others'[18].

## References and Notes

[1] The meaning of the terms 'privacy' and 'data protection' have been keenly contested by lawyers and academics alike. Very broadly, 'privacy' is perceived as a wide value covering bodily privacy, territorial privacy, privacy of communications and information privacy. It is the latter value, also known as 'data protection', that is investigated in this thesis. This debate is discussed in further detail in Chapters 3 (Literature Review) and 4 (Data Protection and the Law).

[2] Naturally, exemptions from certain provisions of the DPA 1998 exist for various purposes. They include national security, crime and taxation, health, education and social work. The main exemptions appear in Part IV of the Act.

[3] Refer to discussion in Chapter 4 (section 4.6).

[4] Refer to discussion in Chapter 6 (section 6.2.3).

[5] Refer to discussions in Chapter 6 (section 6.2).

[6] Refer to Chapter 7 (section 7.5).

[7] Over half the respondents (63, 58.9%) had devised policies for handling subject access requests, yet only 32 respondents (29.9%) had specific policies in place regarding employee access to their personal data. The methodology and findings from the questionnaire survey are discussed in Chapters 2 and 6 respectively.

[8] Refer to case study analysis in Chapter 7 (section 7.5).

[9] *Ibid.*

[10] The findings from the questionnaire survey and case study interviews are discussed in Chapters 6 and 7 respectively.

[11] Great Britain. *Freedom of Information (Scotland) Act 2002.* London: TSO.

[12] For detailed list refer:

- *Ibid.*, schedule 1.

[13] Following the terrorist attacks in the United States, legislation increasing the powers of domestic law enforcement agencies has been passed by a number of Western governments. In the UK, the *Anti-Terrorism, Crime and Security Act* was enacted in December 2001. The data protection implications of this statute are discussed in Chapter 5 (section 5.5.3).

[14] Westin, A.F. *Privacy and freedom.* 1967.

[15] Rule, J.B. *Private lives and public surveillance,* 1973.

[16] The observations and findings of the vibrant research community into data protection permeate the entire thesis. Most attention is given to academic research in Chapters 3 and 4.

[17] The methodology involved in selecting and interviewing these individuals is discussed in Chapter 2. The findings from the interviews are analysed in Chapter 6.

[18] Westin, A.F. ref. 14, p. 7.

# 2. Methodology

## 2.1 Introduction

### 2.1.1 Research methodology texts

Various texts were consulted concerning general research techniques. Usually the texts were located from the author's reading, although some were the result of personal recommendation of academics at Loughborough University's Department of Information Science. For a general overview of academic research methodologies, Bell[1] proved a helpful reference companion. Aimed at students, *Doing your research project* assumed no prior knowledge of research methodology, and provided a step-by-step guide through the research process from choosing a topic, to collecting and interpreting data, to writing a final report. Other useful guides included Denscombe[2] – focusing on small-scale research projects – and Moore[3] – aimed not just at academic researchers, but also those working in government and industry.

Gorman and Clayton[4] assessed qualitative research – the approach largely used in this thesis. The authors identified its key features and considered the advantages of triangulating this method with other research approaches. The process of triangulation, defined by the authors as the use of 'multiple methodologies'[5], is analysed in sub-section 2.1.3 of this Chapter. Additionally, Gorman and Clayton considered the mechanics of using case studies, described as 'the application of specific qualitative research methods in a specific setting'[6]. Interview case studies – a key part of the research methodology employed in this thesis - were seen as particularly pertinent, with the authors emphasising that interviewee responses should be allowed to drive the interview process forward. Further analysis of case study methodology has been produced by Yin[7]. The author considered the theory, design and evaluation of case studies, giving various examples that ranged from education to computer software development.

Other academic texts considered specific elements of the research process. Hart[8] provided an excellent detailed analysis of the literature review, defining its role in research broadly:

> 'To demonstrate skills in library searching; to show command of the subject area and understanding of the problem; to justify the research topic, design and methodology.'[9]

Hart considered the analytical pattern of the literature review, the importance of the researcher choosing an appropriate structure for their argument, and the practical benefits of the review in progressively narrowing down a topic. Fink[10], additionally, provided a guide to actually conducting the literature review – demonstrating how to identify, interpret and analyse published and unpublished research.

Numerous texts existed concerning the conduct of questionnaire surveys and interviews. For the former, practical guides by Fink[11] and Youngman[12] – whose definition of question type is considered in section 2.3.1 – were consulted, in addition to relevant chapters in Bell[13] and Denscombe[14]. Concerning the interview process, Bell[15] and Gorman and Clayton[16] proved helpful, not only outlining the structure and purpose of interviewing, but also emphasising the need for honesty and integrity - in particular respecting requests for anonymity and not taking advantage of any indiscretions on the part of the respondent.

The texts referred to in this section gave ideas about building a general methodology, which could be applied to the specific research topic of this thesis. The research process as a whole was outlined, and particular methods highlighted. However, in order to construct a methodology for assessing data protection, it was important to consider detailed research projects that have already been conducted in this field.

## 2.1.2 Developing a methodology

Assessing the effectiveness of legislation and policy was not an easy task – relying more on qualitative than quantitative analysis. To some extent, the authors of some of the most significant studies in this field have relied on a mix of qualitative techniques. Examples include: documentary analysis – in particular business and government reports, plus material from privacy advocacy groups (Cate[17]); comparative analysis of the data protection statutes (Nugter[18]); expert interviews with civil servants, lawyers and civil libertarians (Flaherty[19]); and case studies concerning public and private bureaucracies' processing of personal data (Rule[20]). Most scholarly research has combined some of the above techniques, with authors employing a difference in emphasis. Other equally fundamental texts are discussed in the literature review that is Chapter 3.

A methodology for conducting an evaluation of data protection legislation was developed by Raab and Bennett during the mid-1990's[21]. The authors decided on key criteria that could be used objectively to facilitate an evaluation of the data protection system as a whole:

(i) The law itself;

(ii) The performance of the supervisory authority, for example, dealing with complaints, prosecutions, production of information booklets;

(iii) The performance of the data controllers in adopting best practice;

(iv) The performance of the data subjects in taking steps to protect their personal data - for example, by removing their names from mailing lists or requesting access to their own data.

This PhD study had to set boundaries – lacking the time and resources to research into such detail. Nevertheless, desk research and fieldwork touched on three of the above criteria to some degree. Legal clarity and policy are analysed in Chapters 4 and 5. The performance of data controllers, in this case public authorities, in adopting best practice is considered in the case studies. However, awareness and performance of data subjects – certainly an interesting and important subject area – has not been considered due to the aforementioned constraints.

Raab and Bennett drew the following conclusions regarding a sound data protection methodology:

(i) Criteria for assessing performance were difficult – one needed to focus primarily on the activities of the data protection agency and the political processes that drive it;

(ii) The only reliable criteria were procedural – rules, codes, sanctions and decisions. Evaluate on the basis of whether the system adequately puts in place procedures for data subjects to exercise their own privacy rights (for example, to enable subject access requests);

(iii) Data protection agencies needed to define their own system of performance measures and regularly test them;

(iv) Policy implementation within organisations required a 'bottom up' perspective. Procedures achieved at ground level through negotiating, bargaining and influence should be observed, rather than relying solely on quantitative goals imposed by senior management.

Raab and Bennett emphasised qualitative measures in the evaluation of data protection policies. This allowed for some promising avenues of research, particularly in the field of comparative policy analysis. The ultimate outcome of a successful data protection policy would be, to quote a UK data protection official: 'that we should work ourselves out of business if all data users were doing everything absolutely properly and complying with the data protection principles.'[22]

At the same time, the European Commission was developing a methodology to measure 'adequacy' of protection governing personal data transferred to 'third countries', that is, countries outside of the scope of the EU Data Protection Directive[23]. The Commission's early findings were published in a 1997 working paper[24]. Although the context to this methodology is different, the content is relevant to the criteria for compliance outlined in Chapter 7 (section 7.1.2) of this thesis. In particular, the working paper stated:

> '...any meaningful analysis of adequate protection must comprise ... two basic elements: the content of the rules applicable, and the means for ensuring their effective application.'[25]

The 'content' element of the methodology comprised six core principles, a shorthand version of the eight data protection principles that appear in the UK DPA 1998. The second half the statement refers to the procedural and enforcement mechanisms available in the third country. They need not be embodied in national laws, as in EU member states, but must: ensure a good level of compliance; support and help individual data subjects; and provide appropriate redress. This could be achieved through codes and sanctions, verified by auditors or independent data protection officials. Compensation could be paid through a system of independent arbitration.

This methodology was applied by Raab *et al*, in an EU-commissioned study assessing adequacy of the level of protection of individuals regarding the processing of personal data in six non-EU countries[26]. Five categories of data transfer were analysed: sub-contracted data processing; human resources data; medical data; electronic commerce data; and sensitive data in airline reservations. Reporting in 1998, the authors argued for 'a more empirical analysis of policies and practices, as well as rules', in order to assess implementation of principles outlined in the Directive by data controllers[27]. This could be facilitated by the use of certifiable privacy standards, a process that would involve 'proper self-regulation and regular compliance auditing'. The Canadian scheme, mentioned in Chapter 4 (section 4.7.2) of this thesis, was given as an example[28]. Thus it was important to consider both the policies and practices of specific organisations, in addition to 'the broader regulatory environment'. Raab *et al*'s study concluded with an inventory of research questions – used as a guide for data collection, and useful for anyone researching data protection compliance[29].

The above recommendations concerning policy implementation within specific organisations have been taken seriously in this thesis. As a result, this study chose case studies, focusing on public authorities and paying particular attention to policy in practice. In certain respects, this case study methodology owed a little to

Rule's approach in his classic work *Private lives and public surveillance*[30]. Rule's study - discussed in Chapter 3 – relied mainly on semi-structured interviews and direct observation to investigate the collection and use of personal information in organisations such as the UK Driver Licencing System and the US Consumer Credit Reporting System. Rule's case studies were organised using the following strategy[31]:

(i) *Structure of organisation*:

- Account of the human organisation of the bureaucracy;
- Discussion of the structure of the information kept on the system's files, with regard to both form and content.

(ii) *Movement of information and decision-making – the processes involved*:

- Movement of data into files kept by the system;
- Movement of data within and without the system, and how this bears on decisions made for administrative efficiency;
- Relationships between management and staff;
- Question of employee privacy versus administrative efficiency.

(iii) *Patterns of change (in the case of this study orchestrated by the DPA 1998)*:

- Guidance from the top – for example, government and the OIC;
- Internal guidelines – are there any improvements/recommendations in store for the immediate, foreseeable future?

Although Rule's methodology was aimed at analysing the collection and use of personal data by large organisations as a means of centralised surveillance on broad sectors of the population during the early 1970's, it provided a useful template for this study concerning the procedures used by public authorities to safeguard personal data of employees and the general public.

## 2.1.3 Triangulation of research

The thesis achieved its aims, outlined in Chapter 1, through triangulation of research. Lines of enquiry opened up through desk research have been backed up by fieldwork, resulting in the structure in Figure 1 overleaf.

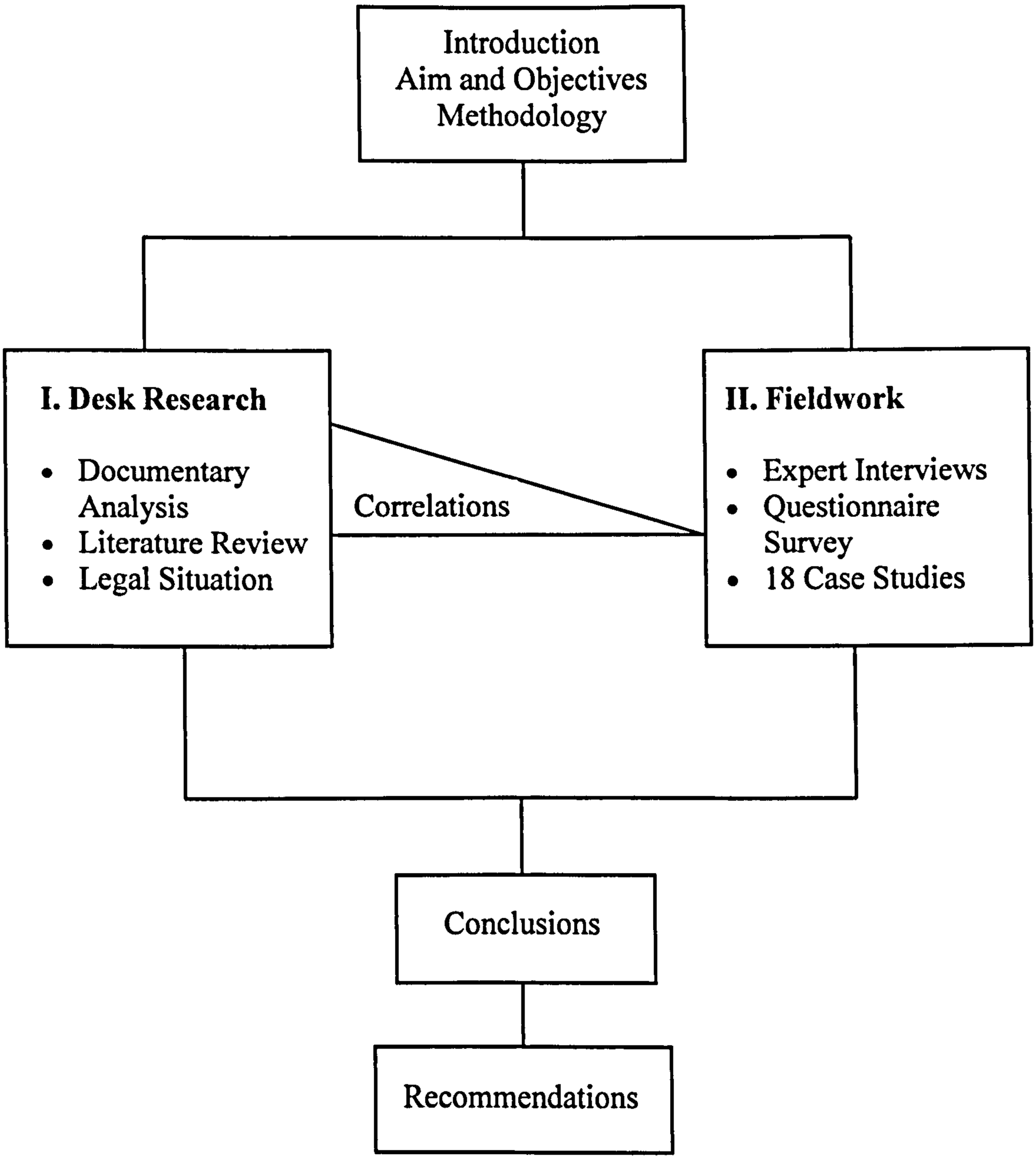


Figure 1: Triangulation of research

This multi-method approach involved cross-checking, or corroborating, the existence of certain trends and the reliability of individual accounts by gathering data from a number of informants and a number of sources. The above diagram displays the generic approach taken. At ground level, each method was as far as practicable compared and contrasted with two other inputs of evidence to produce as full and balanced a study as possible. For example, the findings generated by the documentary analysis and literature review were cross-validated by expert interviews. Evidence from questionnaires and research into legal context were compared to the accounts given during in-depth case study interviews. Ultimately, the viewing of accounts from different perspectives - together with the opportunity to corroborate findings -

enhanced the validity of the data.

Such an approach, however, had to be weighed against time constraints. Moreover, the findings have been affected by the willingness of people to be interviewed, to complete questionnaires and, in case study scenarios, to be interviewed in further depth. The findings are discussed and disseminated in detail in Chapters 6 and 7.

The data collection procedures were assessed for their reliability and validity. Reliability referred to the extent to which the methods produced similar results under constant conditions, on all occasions. This was particularly important for questionnaires, where checks for reliability came at stage of question wording and piloting of questionnaire survey with sympathetic and expert parties recommended by staff in the Department. Validity in the context of this project referred to the soundness of the methods employed – do the methods measure or describe what is supposed to be measured or described? Are the correct methods being used? At the piloting stage, the validity of the questionnaires was tested, ensuring the questions were clear and unambiguous and that the survey was indeed measuring what it was intended to measure. Further discussion of the piloting process can be found later in this Chapter, and in Chapter 6. The findings for a sample of the questionnaires were probed deeper during the in-depth follow-up interviews, analysed in Chapter 7.

Reliability and validity were also factors during the interviews – particularly in relation to questions of historical and legal nature. Following transcription of interviews, documentary evidence such as government policy papers, Committee reports and case-law reports – often dating back thirty years – were revisited to follow up points made by the interviewee and verify information imparted. Frequently, this resulted in additional insight gained from the interviewee. The approach throughout was empirical and functional – seeking to understand the practicalities facing organisations. Priority has been given to understanding the reality as opposed to the language of the relevant statutes. Interviews continually opened up new insights - and documentary evidence - from which further information was gleaned.

## 2.2 Desk research

The desk research took two forms – documentary analysis and a literature review. This research helped define what was important, controversial and unique about the topic. It enabled statements to be made that could be tested during the fieldwork stage. Moreover, it demonstrated how questions raised had been addressed in the past, and indicated what may be missing, and consequently, where any scope for original research may lie. The outcomes of the desk research are found in: Chapter 3 - the detailed literature review; Chapter 4 - investigating the legal context to the DPA 1998; and Chapter 5 – assessing the wider legal context.

### 2.2.1 Documentary analysis

Documentary analysis involved studying various legislation, policy papers and discussion documents from the UK and abroad. They covered a time span of thirty years from the early 1970's to the present day. This approach provided a solid foundation for the fieldwork questionnaires and interviews, aiding in the formulation of key research questions. A document search was undertaken to ascertain the existence of different sources of information. This was conducted using a variety of methods. The first mention of a document was often in the notes and references to various academic articles and books studied for the literature review referred to in Chapter 3. Electronic databases proved invaluable research tools, enabling the rapid retrieval of a particular document. Among the most used databases were BOPCAS – detailing full bibliographic references to UK official publications by The Stationery Office, and the *Eurolaw* database – giving full text access to European Union (EU) Treaties, Directives and Regulations. Hard copy insights into UK and EU decision-making processes were provided by *Hansard* and the *European Union Encyclopedia and Directory* respectively. Where the databases failed to locate a specific document, academic librarians at

Loughborough University's Pilkington Library in particular proved unfailingly helpful.

Publications from membership organisations such the Confederation of British Industry (CBI) and the Trades Union Congress (TUC), plus various non-Governmental Organisations (NGOs) such as JUSTICE and Consumers International, were often available on their Internet websites. Where this was not the case, most bodies were able to post out documents on request.

There were inevitably some frustrations when conducting the document search. For example, permission was sought from the Home Office to acquire the original papers from the 1976 Data Protection Committee from the chairman, Sir Norman Lindop, who was willing to dispose the documents. However, this was denied, on advice from the Public Record Office - which stated that it should be the true repository of such documents, and re-iterated that some of the papers detailing, for example interviews and submissions by the police and secret services, were to remain closed for thirty years[32]. Such documents would have proved valuable as evidence as to the secretive culture within certain public organisations at a time when data protection issues were beginning to raise public concern[33]. However, that proved to be only a minor setback. On the whole, government departments, Parliamentary Committees and the European Commission were happy to make documents available.

The documents were analysed to determine what was said, who wrote it, and why it was written. Additionally, consideration was given to how the source came into existence, whether it was typical of its kind, and the audience for which it was written. Documents were compared to other sources of information – such as the views of interviewees – to verify their accuracy and whether such evidence was reliable. In certain sources, bias was an important characteristic. This was often the case with documents from NGOs, trade unions and employers' organisations such as the CBI. Authors of such documents often had a stake in pursuing a particular course of action which affected their views on certain legislation or policy. In some cases, the most useful evidence derived from such sources - providing valuable insights into the political processes involved in policy-making.

Such evidence, although not necessarily an accurate account of a development in policy or technology, was a reliable expression of the author's views. Such analysis enabled a fuller appreciation of the worth of such documentary evidence.

### 2.2.2 Literature review

A critical survey of the available literature was conducted – from academic journals to the quality press, from conference papers to monographs. This survey provided ideas about other approaches and methods: aiding analysis and interpretation of documentary data, and providing a useful template for the formulation of guidelines in the concluding Chapter. Data protection policy is fluid, and references soon date. Research tools used to locate the most recent publications included: newspaper databases on CD ROM, for example *The Guardian* and *The Times*; and electronic resources such as ASSIA Plus, CSA and Web of Science for academic articles. Those tools yielded a large amount of information under basic search terms such as 'data protection', 'privacy' and 'European Data Protection Directive 1995'. For EU-funded research, the CORDIS gateway proved a good starting point with nine databases providing access to complete information on the research programmes, in addition to summaries of official documents relating to the EU's legislative and decision-making processes. For comparative information concerning North America, the ABI Research Index was an excellent platform, with an advanced search engine enabling detailed searches on North American business periodicals, academic and educational journals, in addition to articles from newspapers such as *The Washington Post.*

### 2.2.3 Current legal situation

Chapter 4 analysed the present, conflicting, legal situation in detail. The historical context to data protection law in particular was significant to the type of data protection regime chosen by the UK. Consequently, the Chapter described the context to current information privacy law in some considerable detail, drawing on

legislation and policy documents from the last thirty years. References were made to other countries to highlight the diversity of international policy is in this field, and shed some light on the difficulties in providing data protection in the current political and economic climate.

The inherent problems in legislating for data protection were investigated. In particular, the difficulties presented by emerging technologies such as genetic testing and sophisticated workplace performance monitoring were considered. Additionally, the implications of other UK legislation impacting on data protection have been examined. Key legislation included: HRA 98; FOIA 2000; FOI (Scotland) Act 2002; and RIPA 2000. The relationship between such diverse laws is key in investigating whether a viable data protection regime can exist in the UK.

### 2.2.4 Other research in the field

In addition, contact has been maintained with academics and practitioners working in the field. Emails have been exchanged and contributions have been posted to the JISCmail data protection discussion list[34]. Finally, the author attended the following relevant conferences, either as a delegate or speaker:

- *Keep IT Legal 4th Annual Conference,* Nottingham. May 2001 (delegate);
- *10th international BOBCATSSS symposium on library and information science*, Portoroz, Slovenia. January 2002 (speaker)[35];
- *NADPO*[36] *Annual Conference*, Warwick. November 2002 (invited speaker).

## 2.3 Fieldwork

Detailed fieldwork was largely qualitative, consisting of interviews, questionnaires and case studies. Quantitative methods in a study concerned with policy and best practice were more difficult to justify and consequently have been limited to graphical representation of data concerning compliance with, and opinion

concerning, the DPA 1998 and the HRA 1998. This section outlines the advantages of the qualitative measures used. Three techniques were employed. Firstly, a questionnaire survey, conducted during autumn 2001, aimed at testing practitioner opinion and developing contacts within public organisations. In particular, the survey sought to assess the challenges facing organisations regarding the handling the employee personal data. Secondly, expert interviews – also conducted during autumn 2001 – establishing an overview of opinion on data protection and human rights issues. Finally, case study interviews, performed in spring 2002 with a sample of the bodies contacted during the questionnaire survey.

### 2.3.1 Questionnaire survey

The questionnaire survey was a data collection method that required careful consideration in selection of question type, question writing, design, piloting distribution and return of the questionnaires.

#### *Purpose and design*

Firstly, it had to be decided exactly which data was being sought, and indeed whether a questionnaire was the most appropriate method for collecting such information. Following some deliberation and consultation with supervisors, the author decided a questionnaire could yield some useful indicative data regarding the measures public authorities were taking towards complying with the DPA 1998. Most importantly, the survey could provide an opening for future case studies. The survey was not expected to produce statistically significant findings. The most significant areas for investigation had been identified by preliminary reading and the aim and hypotheses outlined in the introductory Chapter. A deliberate focus was placed on the processing of personal data belonging to employees, reflecting activities in this field by the UK OIC – most notably its publication of a draft code of practice and industry's reaction to it[37]. The questionnaire intended to provide a practitioner view of the draft *Code*, which had been absent from the media debate surrounding the issue.

Subsequently, a sample was determined for the questionnaire survey. It was decided to test the reaction, opinion and measures taken by public authorities to comply with the DPA 1998, HRA 1998 and RIPA 2000. From the outset, it was accepted that the sample was going to be biased. Loughborough University's Library and Information Statistics Unit (LISU) and the JISCmail data protection discussion list were both consulted to provide details of organisations with a particular interest in this field. The main survey was limited to public authorities, as they were unambiguously affected by the provisions of the HRA 1998. Organisations approached included public libraries, local authorities, the police, universities and the National Health Service (NHS).

Based on this information, the questions were drawn up into four clear, though overlapping, areas concerning:

A. Compliance with the DPA 1998;
B. Policies on privacy;
C. Monitoring of employees;
D. Awareness of, and opinions concerning, the DPA 1998, HRA 1998 and RIPA 2000.

Fourteen questions were included. The language was checked to achieve the degree of precision necessary to ensure the subjects understood exactly what was asked. Particular care was taken to avoid leading questions that prompted the respondent to answer in one way (for example: 'do you not agree that employees have a right to free use of internet in the workplace?') or double or triple questions which expected more than one answer.

The question type employed was mainly structured – making answering the survey and analysing the results easier. Four of the seven types of question listed by Youngman[38] were employed in the pilot survey:

- *List questions*, where a list of items was offered, any of which could be selected. For example, concerning the steps an organisation had taken to comply with the DPA 1998;

- *Categories*, where the response was one only of a given set of categories. For example, the frequency with which an organisation monitored staff use of the internet;
- *Scaling*, to measure level of awareness and opinion concerning the various legislation. A Likert scale was used, measuring the strength of agreement/disagreement with given statement on scale of 1-5. Responses could then be presented in tables or bar charts;
- *Open questions*, where the expected response was a word, phrase or extended comment. Responses to verbal questions produced some useful information which could be followed up in later case studies. Others provide pertinent quotations to illustrate certain points in the thesis. In the pilot study, such questions were also important in finding out which aspects of the topic were of particular significance to the respondents.

*Pilot questionnaire*

The pilot questionnaire survey was distributed during February 2001. Essentially, it was an opportunity to test: data collection techniques; timeframe; data analysis methods - removing any items that do not yield useful data; and consider any suggestions for improvement made by the respondents. It was trialled on a group similar to that which would form the population of the study. Organisations sampled included a university, an academic library, an IT company and civil liberties bodies. The university and academic library represented public authorities, whereas the IT company was included for variety, and because at that early stage of the project the author was still debating whether to include the private sector. Four civil liberties bodies were sampled. In part, this was to achieve some input from bodies campaigning for data protection and human rights; in part, it was to aid preparation for later fieldwork interviews with these bodies.

As participant feedback was the key objective of the pilot, a form was attached to the survey with the following questions[39]:

(i) How long did it take you to complete?

(ii) Were the instructions clear?

(iii) Were any of the questions unclear or ambiguous? If so, will you say which and why?

(iv) Did you object to answering any of the questions?

(v) In your opinion, has any major topic been omitted?

(vi) Was the layout of the questionnaire clear/attractive?

(vii) Any comments?

The responses enabled revision of the questionnaire in time for the main distribution. Out of the 11 questionnaires issued, seven were returned.

The time taken to complete the questionnaire ranged from 'a couple of minutes' to 30 minutes. The majority took between five and 10 minutes. This was deemed acceptable – long enough to give considered responses, yet not too intrusive on the respondent's work routine. All subjects found the layout and instructions regarding the questionnaire to be clear. However, there was some confusion over the phrasing of two of the four statements measuring strength of feeling in the final section of the questionnaire:

- The *Lawful Business Practice Regulations* complement the *Draft code of practice on the use of personal data in employer/employee relationships*;
- The Human Rights Act will work effectively in tandem with the Data Protection Act 1998. Overlap is minimal and meaning is clear.

The above statements were intended to measure opinion on the diverse official guidance, regulation and legislation concerning personal information. However, one respondent suggested it was unclear whether two documents can 'complement' each other. They could fail to complement each other by being inconsistent, or by addressing entirely different sets of issues. The second statement was deemed unanswerable as it posed three separate questions concerning: the relationship between the HRA 1998 and DPA 1998; degree of

overlap; and clarity of meaning. Finally, one respondent was unclear as to the purpose of the questionnaire – whether it was testing:

(i) Informed opinion on the effectiveness of the various legislation/regulations, or;
(ii) Awareness of the existence and contents of those schemes?

In fact, the survey was testing both. The cover letter accompanying the main questionnaire survey was amended to reflect this, stating: 'this survey will measure awareness and informed opinion concerning the above regulations...'. The feedback from the pilot survey was certainly worthwhile, helping to determine the structure and wording of the full questionnaire.

*Amendments following pilot questionnaire*

Following this feedback, important amendments were made to the questionnaire format, as detailed below:

- Part 1: *Compliance and staffing* – reducing section A of the pilot to just two questions;
- Part 2: *Employee records* – this amended section B of the pilot, sharpening the focus on employee personal data. This was deemed necessary as part of the process of clarifying the aim of the survey. Questions related to records management issues, comprising: purposes for which personal data was being collected; retention periods of employee records; procedures in place to check accuracy of such records; subject access procedures for those wishing to view their records; and the security procedures in place for safeguarding records;
- Part 3: *Monitoring of employees* – this remained unchanged from the pilot. Respondents appeared to have little difficulty understanding this section;
- Part 4: *Legislation and official guidance* - considered awareness and opinion of current legislation. This section had been modified in line with the feedback. The first question in this section tested the awareness of legislation and guidance with simple 'yes' or 'no' options. The second

question had five instead of the previous four statements concerning strengthen of feeling about the HRA 1998 and DPA 1998; and official guidance. However, each statement was simplified with the final triple statement scrapped, and being replaced by two straightforward statements concerning official guidance to the DPA 1998 and the HRA 1998.

Finally, a box was added for contact details for those interested in participating in follow-up case study interviews later in the academic year. The revisions, especially in Part 2, had the effect of increasing the length of the questionnaire from four pages of A4 paper to five. This was unfortunate, but justified as an attempt to clarify the issues surveyed, yet maintain the logical progression of the questions within the questionnaire. This consolidated the main purpose of the questionnaire: to provide a solid foundation for detailed follow-up interviews.

*The full questionnaire survey*

The questionnaire survey (refer to Appendix D) was distributed to diverse organisations from the public sector – explicitly covered by the provisions of the HRA 1998. The organisations included public libraries, local authorities, health authorities, universities, police authorities and privatised utilities. Privatised utilities were included as they conducted public functions and were covered in that respect by the provisions of the HRA 1998[40]. It was reasoned that contacting organisations known to Loughborough University – via LISU - or those interested in data protection – via the JISCmail discussion list - would improve the response rates. For the privatised utilities, web trade directories (for example, the Electricity Association[41]) and websites of watchdogs (for example, Ofwat[42] and Ofgem[43]) were referred to – resulting in a list of 43 organisations covering water, electricity, gas and transport. Reference to the above sources of information resulted in a list of 382 organisations, broken down into the following categories:

| Type of organisation | Number of questionnaires posted |
|---|---|
| Local authorities | 258 |
| Universities | 58 |
| Health authorities | 10 |
| Police authorities | 9 |
| Quangos[44] | 4 |
| Privatised untilities | 43 |
| | |
| Total | 382 |

Table 2: Distribution of questionnaires by category.

It was decided that this total was enough to generate indicative findings and, most importantly, permit access for case study interviews.

*Distribution and return of questionnaires*

It was decided at an early stage to distribute questionnaires by post. This was so that the respondents would have a tangible copy which to answer or distribute to colleagues. The survey was printed on coloured paper in an attempt to make it stand out on respondent's desks from other documents. A stamped addressed envelope was included. Two months prior to distribution, the organisations selected were contacted by email in order to give advance notice of the intention to post a questionnaire. Details were given as to the intentions of the survey and the overall context of this thesis, together with a link to the author's research website[45] and personal contact details. Developing a relationship with the respondent was seen as key to improving the response rate and, more importantly, willingness to participate in follow-up case studies. Moreover, advance notice allowed organisations to opt-out of the study – saving time and resources at a later stage. However, the number of early refusals was outweighed by the nine public authorities that indicated their readiness to fully participate in the study, and the interviews before even receiving the questionnaires. At such an early stage, that was an encouraging response.

The questionnaires were posted out with an accompanying letter. This letter stated the purpose of the survey and how any information provided would be processed. Confidentiality was promised. Nevertheless, each survey was given a general identification (ID) number to track response rates. This was felt necessary to avoid duplication and irritation when the time came to pursue non-respondents. However, this ID number was meaningless unless one had access to the coded list of the organisations contacted. In fact, confidentiality did not appear to be an issue with respondents, and many questionnaires were returned with business cards or compliments slips attached. Nevertheless, the names of the respondents have not been included in the thesis.

The survey was sent out during the first full week of September 2001. A return date of five weeks following distribution of all the surveys was given. This was deemed reasonable – as less than a month might have appeared pressurised, and any longer might have tempted respondents to put the questionnaire to one side, decreasing the chances of getting as response. The precise day and date of return were stated in the cover letter, and prominently displayed on the questionnaire.

The ID number helped track the response rate, discussed in detail in Chapter 6. Following the passing of the deadline, it was decided after some debate between the author and supervisors to pursue non-respondents. A number of options were considered, then discounted. Posting out follow-up questionnaires to all the organisations that had not replied would have proved prohibitively expensive. It would also likely have proved futile, as a subject who has already declined one postal questionnaire is unlikely to complete a second such survey. Emailing non-respondents was considered too much of a scattergun approach. Besides, email addresses were not available for a considerable number of the original sample.

It was finally decided to telephone the organisations involved. This had the advantage of communicating directly to the subject and finding reasons for non-response. Additionally, it allowed follow-up surveys to be targeted at those who needed them, thus saving resources and improving the response rate. Approximately 250 organisations were contacted by telephone. Although systematic, the procedure proved protracted as, in the period of three months, a

number of respondents had changed jobs. In other cases, telephone numbers had changed. It proved particularly difficult to locate the relevant person within local authorities – each having its unique corporate structure – and it was not uncommon to be channelled through three different departments before speaking to the named respondent. Nevertheless, the process was instructive, yielding useful anecdotal evidence of the reasons for non-response. Some of the reasons are given below:

- The questionnaire was found by some to be too complex. taking up too much time;
- Pressure of other work – particularly in libraries where the appearance of the survey coincided with the book-ordering season;
- Staff shortages;
- 'Survey overload', with some organisations receiving 4-5 surveys a week;
- The questionnaire, particularly in local authorities. having circulated various department – IT, legal, and human resources were most frequently mentioned - before inevitably being mislaid;
- The organisation having a specific policy of not responding to student surveys;
- The respondent had not received the survey;
- The contact had left the organisation, and no-one else had responded to the survey.

The uncertain location of the data protection function within organisations compounded the issue – with departments as diverse as corporate services, IT, legal, administration and finance all claiming some responsibility. Often, the designated individual had duties other than data protection. This exacerbated the difficulties in targeting the questionnaire in the first instance, and hindered the pursuit of non-respondents.

However, the contacting of non-respondents by telephone did have a positive effect. As a consequence of the calls, 60 further questionnaires were posted - and eight emailed. Of those, nearly 50 were completed and returned.

### 2.3.2 Expert interviews

The value of interviews with experts in the field and those from particular interest groups was recognised at an early stage. A semi-structured format was chosen. Its key advantages were perceived as:

- Enabling subjects to talk at length, eliciting detailed information;
- Shedding light on a sensitive topic in a way a written response may conceal;
- Allowing questions to be asked that cannot be answered elsewhere;
- Triangulating desk research by following up specific lines of enquiry.

Initially, a list of questions was devised around a loose structure to ensure all the topics were covered. Some of the questions were generic – based on issues raised during desk research, and the pilot questionnaire. Common questions concerned:

- Interviewee's role in that particular organisation;
- Aims of the organisation;
- When and how that organisation developed an interest in data protection and/or human rights;
- Other bodies consulted/extent of peer group cooperation within this field;
- Official and personal opinion on current legislation.

One of the key aims of the interviews – other than establishing opinion – was to understand the processes and relationships that existed in the field of data protection and human rights between government, NGOs, business, trade unions, supervisory authorities and Parliament. Further questions were tailored specifically to the organisation or individual concerned – usually concerning a particular piece of research conducted by that body. Where possible, the interviewee was emailed the questions in advance, in order to prepare for the interview, and if necessary come back with any queries – although that did not

happen. Within this framework, the respondent was allowed a considerable degree of latitude. Certain questions were asked, but the subject had the freedom to talk about the topic and give their own views in their own time. This approach was largely successful, with the interviewee usually moving from topic to topic with little prompting. With such a flexible format, the length of time for the interviews varied considerably – ranging from 20 minutes to two hours. Generally, the average time taken was 50 minutes.

The respondents were selected on the basis that they would have something significant to contribute to the field. They were considered experts with experience in policy making, law or campaigning. Interviewees were identified in a number of ways: during the piloting of the questionnaires; from published research; conference speeches; and, in one case, on the recommendation of one of the author's supervisors. Initially, the proposed interviewees were approached by letter or email during July and August 2001. As with the communications prior to the questionnaire survey, details of the research and the desired outcomes of an interview were outlined. Additionally, a link to the author's website and contact details for any queries were provided. Finally, the use to which the information would be put was summarised – allowing the interviewee the opportunity to remain anonymous if preferred.

Of the 30 people and institutions approached, 15 agreed to be interviewed. Only four failed to reply at all. The reasons given by those who declined to be interviewed were:

- Time constraints;
- Not having conducted any relevant research into the field;
- Having a policy of not participating in student research.

Sample interview transcripts can be found at the end of this report. The people approached included civil servants, lawyers, trade unionists, business, regulatory bodies and NGOs.

Good time management was essential when planning for the interviews. Account was taken of time required for planning and conducting the interviews, for coping with delays and, particularly in large organisations, being shuttled from one contact to another. In all cases, permission was requested to tape-record the interviews. This was considered most appropriate for the semi-structured format, where responses could not always be easily analysed. Of the 15 interviews conducted, 10 were tape-recorded. One respondent was unable to be interviewed due to illness, but completed an email questionnaire at a later date. A second respondent also completed such a questionnaire – due to time and resource difficulties in arranging an interview overseas. Of the three face-to-face discussions not tape-recorded, only one individual specifically refused permission. In the other two instances, office conditions meant that tape-recording was not feasible. In those cases, notes were taken and written up as soon as possible after the interview ended.

Tape recordings proved useful for checking the wording of any statement prior to quotation, and invaluable for content analysis. Where possible, interview transcripts, particularly statements to be used as direct quotations in the report, were verified with the respondent. Permission to publish the transcript was sometimes asked at the interview stage, or failing that, by letter following transcription. Only one of the 10 tape-recorded interviewees refused permission for the transcript to appear in the thesis.

Analysis of the results and quotations from the interviews are included in Chapter 6.

### 2.3.3 Case studies

The most fundamental part of this project, the case studies had the clear advantage of allowing a number of public organisations to be studied in depth. Following the questionnaire survey, 19 public authorities stated their intention to be studied in depth, with 18 actually participating in the interview process. They comprised: 12

public authorities; three universities; one health authority; one police authority; and one 'other' – a central government educational organisation.

Again, the interviews were semi-structured, and lasted anything from 40 minutes to two hours. A common approach was taken to all organisations involved. The substantive background to the case studies analysed the nature of the organisations, their corporate structure, and the number of people they serve. The interviews explored questions raised by those affected by the legislation on a daily basis. The emphasis was placed on detail, with hard examples given of any particular measures enacted to safeguard data protection. The key aim of the case studies was to test hypothesis 1. Particular emphasis was given to the workability of the DPA 1998 – as a measure for ensuring compliance and good practice, and that it worked in tandem with the other aforementioned legislation impacting on data protection. Based on earlier research, the author devised the following criteria for compliance:

(i) *Status of the data protection function* in the organisation: are the DPOs being listened to?

(ii) *Public awareness*: informing those outside the organisation of their rights under the DPA 1998 at point of collection;

(iii) *Staff awareness and training*: if employees handling personal data are not trained, organisations cannot conduct their obligations under the DPA 1998;

(iv) *Handling subject access requests (SARs)*: a key aspect of the DPA 1998 in allowing individuals to exercise their rights – verifying what is recorded about them and the basis of decisions taken. How do organisations handle requests from staff and the public for personal information?

(v) *Data protection policy*: do organisations have an overarching policy? How effective is it? What guidance underpins the policy? How is policy evaluated?

The case study interviews were conducted from February to May 2002, and the data is analysed in Chapter 7. The focus has been on the extent to which the above

issues had been given previous thought and how far data protection is built into organisation's policy processes. Finally, Chapter 8 considers the extent to which the aim of the thesis has been achieved. Recommendations – presented to a number of case study organisations – are proposed for good practice.

## 2.4 Limitations of this study

Although this thesis has followed a rigorous methodology based upon triangulation of research, it has faced limitations. The most obvious restrictions have been time and resources. The need to complete this study within three years, and the paucity of funding available, has limited the number of organisations that could be visited. It has also impacted on the depth of research that could be conducted at these organisations. Additionally, the number and location of the experts visited was similarly restricted. However, the author believes a sufficient cross-section of individuals from different sectors – trade unions, business, consumer groups, government and so on - have been interviewed, resulting in an indicative insight into the diverse views concerning data protection.

Moreover, the sheer scope of the DPA 1998, and its related legislation, resulted in limitations being placed on what could be investigated. The organisations interviewed performed a wide range of functions on which data protection impinged. They included: health data and *Caldicott*; police intelligence; education and the role of schools as data controller; exam results in schools, further and higher education; the pastoral role of university tutors; contracts with overseas offices; and the role of local authority councillors wishing to use personal data for political purposes. This list is not exhaustive, and any one of those functions could have justified a significant research project in its own right. Consequently, the decision had to be made to gain an *overview* of data protection compliance procedures in various public organisations to prevent this research project from becoming too bogged down in detail. By the same token, it was vital that this study was not superficial. Hence, the importance of triangulation of research, and receiving feedback from the participating organisations. The latter was achieved through a conference paper presented to NADPO in November 2002[46].

A further limitation was the author's reliance on the information given by the DPOs. Although there was no reason at all to doubt the honesty and integrity of all those interviewed (indeed, the candour of some interviewees was quite surprising and refreshing), there was generally no method of verifying that the changes they claimed to implementing were indeed being carried out, and had been successful. Nevertheless, the author was usually given copies of policies and procedures, and on occasions permitted to speak to other employees in the organisation. The DPOs were busy people, and the fact that they were prepared to give up an hour or two of their time was appreciated. However, if this project had more time, return visits would have been organised and interviews conducted with other employees at differing levels in the organisations. This would have established the full extent to which data handling procedures were in action, and being adhered to.

Subsidiary to the latter point is the necessary caveat that, in general, only those organisations that were well-advanced in terms of data protection compliance were likely to invite the author to interview. Although this can be perceived as a flaw in the methodology, the fact that the author was able to assess almost full data protection compliance (no organisation claimed to be completely compliant) was beneficial to the research conducted, enabling recommendations to be drafted that could be pitched at all levels. The recommendations are outlined in Chapter 8. Moreover, there were certainly two case study organisations – the health authority and a county council - where data protection issues were only beginning to be addressed. The honesty, and perhaps courage, of these organisations in volunteering for interview was greatly appreciated. Thus although it is acknowledged that the sample of case study organisations may be skewed towards those 'doing well' in terms of data protection compliance, this was not exclusively the case.

Additionally, the topicality of subject presented some difficulties. Most obviously, the events of 11 September 2001 caused major changes in the drafting of the legal Chapters (Chapters 4 and 5) and impacted on the nature of the discussions with experts during that autumn. Additionally, the *Employment Practices Data*

*Protection Code* has been under consultation and review for almost the entire length of this project – with the first draft being released in October 2000, and at the time of writing (January 2003) there are still two parts that have yet to be finalised. This has contributed to uncertainty among organisations regarding best practice when monitoring employee communications.

Finally, fresh newspaper reports, emerging academic research and almost frenzied government activity in this field has resulted in the need for the literature review and legal chapters to be constantly reviewed and updated. Of course, this is reassuring – a measure of the relevance of data protection as an issue of public policy and a tribute to the vibrancy of academic research into this expanding field. However, the sheer quantity of output on data protection has resulted in necessary omissions of potentially significant issues – for example, the impact of the DPA 1998 on the private sector - being forced on the author. Discussion of other important activities, for example data sharing between government departments, has had to be minimised. A number of these issues have been flagged in Chapter 8 as topics for further academic research.

## 2.5 Conclusions

The methodology used in this study had its roots in other work – particularly Rule, Raab *et al*, and Raab and Bennett, all cited above. Those works emphasised the need to understand the organisations studied – particularly their structure and the processes involved in information handling and decision-making. It is only by appreciating the movement of data within the system, and the relationships within that structure – between departments, between staff and management - that a thorough critical analysis of the DPA 1998 in action can be achieved.

This study intended to – and hopefully succeeded in – developing some of the issues identified by the above researchers, as well by other academics in this field. Desk research and expert interviews allowed a wide appreciation of the key data protection issues facing organisations. They presented an overview – encompassing the opinions of civil servants, lawyers, business leaders, trade union

representatives and civil libertarians. The questionnaire survey provided a gateway for the case studies – permitting an insight into the data protection issues facing organisations on a daily basis. Finally, the case studies expanded the survey's findings, focusing on the detailed policy and political processes affecting the protection of personal data. In this Chapter, a framework for evaluation has been established – assessing the strengths and weaknesses of internal data protection policies in order to assist public organisations in their policy-making and implementation.

---

## References and Notes

[1] Bell, J. *Doing your research project*. 3rd edition, 1999.

[2] Denscombe, M. *The good research guide*, 1998.

[3] Moore, N. *How to do research*. 3rd edition, 2000.

[4] Gorman G.E. and P. Clayton. *Qualitative research for the information professional*, 1997.

[5] *Ibid.*, p. 32.

[6] *Ibid.*, p. 50.

[7] Yin, R. *Applications of case study research*, 1993.

[8] Hart, C. *Doing a literature review*, 1998.

[9] *Ibid.*, p. 13.

[10] Fink, A. *Conducting research literature reviews*, 1998.

[11] Refer:

- Fink, A. and J. Kosecoff. *How to conduct surveys: a step-by-step guide*. 2nd edition, 1998;

- Fink, A. *How to design surveys*, 1995.

[12] Youngman, M.B. Designing and using questionnaires in Bennett, N., R. Glatter, and R. Levacic (eds) *Improving educational management*, 1994, pp. 248-266.

[13] Bell, J. ref. 1, pp. 118-134.

[14] Denscombe, M. ref., 2, pp. 87-107.

[15] Bell, J. ref. 1, pp. 135-146.

[16] Gorman G.E. and P. Clayton. ref. 4, pp. 124-141.

[17] Cate, F.M. *Privacy in the information age*, 1997.

[18] Nugter, A.C.M. *Transborder flow of personal data in the EC*, 1990.

[19] Flaherty, D. *Protecting privacy in surveillance societies*, 1989.

[20] Rule, J.B. *Private lives and public surveillance*, 1973.

[21] Raab, C.D. and C.J. Bennett. Taking the measure of privacy: can data protection be evaluated? *International Review of Administrative Sciences*, 1996, 62 (4), pp. 535-556.

[22] Great Britain. Home Affairs Committee. *First report: annual report of the Data Protection Registrar*, Session 1990-1991, HC115, 1990. This quote was cited in Raab, C.D. and C.J. Bennett, *Ibid.*, p.554.

The term 'data user' was used under the Data Protection Act 1984 to refer to the organisation or individuals actually processing personal data. In the 1998 Act, this was replaced by the phrase 'data controller'.

[23] European Communities. Commission. *Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.* Official Journal of the European Communities. No. L281/31. (23/11/95).

Article 25 (1) of the Directive prohibited transfers of personal data to third countries unless they ensured 'an adequate level of protection'.

[24] European Communities. Commission. DG XV. *First orientations on the transfers of personal data to third countries – possible ways forward in assessing adequacy.* Adopted 26/06/97. (D/5020/97/EN/Final). WP 4.

[25] *Ibid.*, section 3.

[26] Raab, C.D. *et al. Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: test of the method on several categories of transfer.* Final report. September 1998. DG XV.

[27] *Ibid.*, p.200.

[28] Canadian Standards Association (CSA). 1996. *Model Code for the Protection of Personal Information.* CAN/CSA-Q830-96.

[29] Raab, C.D. *et al.* ref 26, pp.207-212.

The research questions were grouped into nine categories:

(i) Nature and circumstances of the transfer;
(ii) Overview of the regulatory environment;
(iii) Purpose limitation, transparency and opposition;
(iv) Data quality and proportionality;
(v) Security;
(vi) Access and rectification;
(vii) Onward transfer restrictions;
(viii) Remedies;
(ix) Accountability.

[30] Rule, J.B. ref. 20, pp. 35-37.

[31] *Ibid.*

[32] The Committee worked from 1976-1978. Therefore, some papers from the final stages of the Committee are not due to be released until January 2009. A copy of the Home Office letter is included in Appendix B.

[33] For further information on attitudes towards data protection at this time, refer to interview with Sir Norman Lindop, Chairman of the Home Office *Committee on Data Protection* (Appendix A).

[34] The JISCmail data protection discussion list is aimed mainly at practitioners in higher education and local authorities. To view the archives, refer to URL: http://www.jiscmail.ac.uk/lists/data-protection.html [Accessed 16/01/03].

[35] The paper was published in conference proceedings:

- Warren, A. Right to privacy? The protection of employee personal data in the UK. *Proceedings: 10th international BOBCATSSS symposium on library and information science*, Portoroz, Slovenia. 28-30 January 2002, pp. 71-79.

[36] National Association of Data Protection Officers. Refer URL: http://www.nadpo.org.uk/index.home.html [Accessed 16/01/03].

[37] Refer to discussion in Chapter 4 (section 4.6).

[38] Youngman, M.B. ref. 12, pp. 248-266.

[39] These questions are suggested by Bell, J. ref.1, p.128.

[40] For the background to this debate, refer to: Wadham, J. and H. Mountfield, *Human Rights Act 1998*, 1998, pp. 36-38.

[41] An industry organisation for electricity companies. URL: http://www.electricity.org [Accessed 16/01/03].

[42] Ofwat is the Office of Water Services. URL: http://www.ofwat.gov.uk [Accessed 16/01/03].

[43] Ofgem is the Office of Gas and Electricity Markets. URL: http://www.ofgem.gov.uk [Accessed 16/01/03].

[44] Quasi-autonomous non-government organisation.

[45] For the author's website, refer URL: http://www-staff.lboro.ac.uk/~lsapw/index.html [Accessed 16/01/03].

[46] Warren, A. Data protection in public organisations. *NADPO annual conference*, University of Warwick, 18-19 November 2002.

# 3. Literature Review

Following the 1995 European Union (EU) directive relating to data protection[1], and the subsequent introduction into the UK of the Data Protection Act (DPA) 1998[2], together with the incorporation of the European Convention of Human Rights[3] (ECHR) into UK law as the Human Rights Act (HRA) 1998[4], a range of research concerning data protection, privacy and human rights has been published. This research has built upon a generation of previous work that commenced in the late 1960's and early 1970's. Recently, studies have been pitched at varying levels, examining – for example – international concerns, European issues and experience within specific sectors of industry.

In this Chapter, the current state of knowledge and research concerning data protection, human rights and the right to privacy within organisations are analysed and discussed. All have some bearing on this project, and in determining whether the new raft of legislation heralds a new privacy culture in the UK; whether the new laws are adequate or, to quote Miller when referring to the US experience thirty years ago, 'a thing of threads and patches'[5]. Whilst focusing on legislation in the United Kingdom, this Chapter draws necessary reference to a number of high quality studies conducted around the world. The literature in this field is vast, and only a limited number can be incorporated into this Chapter. However, it is believed enough have been included to give an overview of the scope of literature and opinion available concerning privacy legislation.

The Chapter has been divided into three discrete sections. In the first, the research sources available for data protection issues are considered. This section identifies a number of landmark studies that have helped define information privacy in the UK and elsewhere. Additionally, sources of information regarding legal text, current awareness and so-called 'grey literature' are discussed and analysed. Finally, reference has been drawn to research and methodologies that have recently or are currently being used to measure and report reaction to, and experience of, the new law.

In the second section, research issues regarding the HRA 1998 are discussed. In comparison to data protection, this topic has not been the focus of significant investigation. However, as discussed and analysed in this section, there has been a growing corpus of academic and legal work, providing a platform for further research in this field.

The final section considers privacy issues within organisations. In particular, there has been considerable uncertainty with the enactment of various 'information society' legislation relating to organisational handling of personal data. This section also outlines various academic and legal studies in this complex area.

Finally, conclusions are offered – summarising the key findings from this literature review.

## 3.1 Data Protection

### 3.1.1 Landmark studies: the 'privacy' debate

Academic studies concerning privacy and human rights have increased significantly over the last four decades. It was during the late 1960's and early 1970's that the concept of information privacy (or data protection), as distinct from other aspects of privacy concerning physical intrusion and surveillance, was developed. Two US publications in particular helped define the issue – *Privacy and Freedom* by Westin (1967)[6] and Miller's *The Assault on Privacy* (1971)[7]. For Westin, information privacy meant the claim of individuals 'to determine for themselves when, how and to what extent information about them is communicated to others'[8]. Miller's definition was more succinct: 'the individual's ability to control the circulation of information relating to him'[9]. Another publication, Rule's *Private Lives and Public Surveillance* (1973)[10] contained an in-depth examination of the collection and use of personal data as a means of social control. Detailed case studies of organisations such as the UK Driver Licensing system and the US Consumer Credit Reporting system examined what

information the systems collected, through what means, who had access to it, how it was used and how such use impinged on the person it related to. In many respects, they were the first detailed case studies of their kind.

From the academic debates of this period, privacy of personal data emerged as a value that could not be taken or misused by government without due process of law. This idea was later developed into a set of best practice principles - both in the US and Europe - ensuring fair processing, minimal intrusion and limited purposes for the use of personal data. It was this informational aspect of privacy that was most profoundly affected by the rapid developments in information technology during the 1960's. Concerns about the increased use of the computer and the setting up of national databanks were growing. In these circumstances, the choice of the individual was seen as central to the concept of data protection - both in allowing physical intrusion and the sharing of personal information. Westin, Miller and Rule were among the first commentators to articulate and promote such individual choice.

### 3.1.2 Comparative research

As western countries began to enact data protection legislation during the 1970's and 1980's, comparative studies of national laws emerged. The work of Burkert, Nugter, Flaherty, and Bennett were particularly significant in comparing the development of data protection laws during the 1980's, and early 1990's. Burkert and Nugter both provided overviews of data protection legislation within the European Community (EC)[11]. Burkert probed the 'functions' of such laws – that is, the services data protection laws provided for society and the means by which this was achieved[12]. Reconciling basic values – such as access and security – with technological change, and educating all participants in the legislative system, were viewed by the author as particularly significant functions of data protection legislation[13]. Given that such laws were part of a new type of regulations caused by technological changes, Burkert perceived the need for a regulatory mechanism to keep a proper balance between two key objectives:

- Society must adapt to technology to take advantage of the merits of technological change;
- Technology must be adapted to the basic values of society to ensure social coherence in a changing environment.

Burkert highlighted the need to address the all-important role of data protection authorities as new, more specialised public agency and their relationship with more traditional institutions of political power[14]. Although Burkert perceived the data protection authorities 'seem to perform reasonably well', the author optimistically envisioned a time when they could become obsolete, following increased awareness of the value problems of Information and Communications Technologies (ICT), greater openness from data users or controllers, and increased confidence in and access to ICT by individuals[15].

Nearly a decade later, Nugter[16] analysed data protection laws in four EC states as part of a doctoral thesis into the transborder flow of personal data within the private sector. The author concluded that the disparate laws were unable to guarantee sufficient data protection for the data subject where such transborder flows of personal data were involved. As the divergences revealed were obstacles to free trade, Nugter argued that the harmonisation of data protection statutes was obligatory under Community law. The author weighed the options for harmonisation, proposing an EC directive aimed at the highest possible level of protection[17]. It was an indication of the timeliness of this thesis that the year Nugter submitted her work (1990), the EC published its first draft of what became the 1995 Data Protection Directive[18]. The development of a harmonising Directive, with its provisions for judging the 'adequacy' of third country legislation, demonstrated the need for detailed comparative studies, complete with recommendations.

On a wider scale, Flaherty and Bennett published comparative studies of privacy and data protection legislation concerning countries in both Europe and North America. During the 1980s, Flaherty studied the effectiveness of national data protection laws in controlling surveillance, particularly in the public sector[19]. A

hugely significant work, *Protecting privacy in surveillance societies* was one of the first detailed investigations into the work of national data protection agencies[20]. Flaherty articulated their role as bodies that should solely concentrate on data protection. Rather than attempt to develop other aspects of information policy – as happened in France – the agencies should look to strengthen the existing legislation and limit government surveillance[21].

Bennett in *Regulating Privacy* (1992)[22], examined political responses to the data protection issue in four Western democracies, comparing legislation in the US, Germany, the UK and Sweden. This research built on earlier papers[23] where he had contended that, with the definition of privacy being so ambiguous, legislation is most effective if tailored to suit the political and legal cultures of the countries concerned. The author found that five different models existed for the implementation of fair information principles[24]. The law could be implemented through a licencing approach, as in Sweden or France. It could be via a system of registration as in the UK and the Netherlands. Thirdly, it may be administered by voluntary control through self-regulation. Alternatively, the onus could be on the citizenry to enforce their rights in the courts – the 'self-help' solution in the US under the Privacy Act 1974. Finally, the law may be overseen by a Data Protection Commissioner as in Canada and Germany. However, during the 1990's these boundaries, particularly in the EU, became increasingly blurred.

### 3.1.3 Recent academic research 1995-2003

Following the finalisation of the Data Protection Directive by the EU in 1995, a number of general analyses were published - outlining the provisions of the EU Data Protection Directive[25]. Whilst, of course, literature concerning EU data protection initiatives was published prior to 1995, this subsection considers just some of the research conducted since that period. . Opinion on its effectiveness, however, has been divided. Pearce and Platten highlighted the significance of the Data Protection Directive at a European level, as being the first Directive to specifically address human rights issues[26]. In this respect, the Directive represented a landmark piece of legislation for the EU, although the authors

acknowledged that variations in national responses provide major obstacles to achieving to achieving data protection equivalence.

Bainbridge and Pearce argued that in the UK, the DPA 1998 – implementing the Directive into national law - compromised the spirit of the Directive[27]. Whilst the Directive aimed to protect privacy, the word 'privacy' was not mentioned in the DPA 1998. Moreover, in order to benefit from the new data subject rights, individuals had to be pro-active and knowledgeable – directly approaching organisations to object, for example, to direct marketing, and making a complaint to the supervisory authority – now called the Office of the Information Commissioner (OIC) - in case of a breach. The authors were also critical of the enforcement procedures with the absence of custodial sentences for offences, the paltry fines issued by the courts[28] and the small number of prosecutions each year '[doing] little to encourage full compliance with data protection law'[29]. Finally, the issue of consent was brought up, with the authors stating that although various forms of processing are subject to the data subject's consent, it is generally only one of a number of alternative conditions[30]. Thus, 'the data subject's right to prevent processing by withholding his consent is, in the vast majority of cases, merely illusory.'[31]

However, Bainbridge and Pearce believed that the implementation of the HRA 1998 would have a significant impact on data protection law. Article 8 of the ECHR – the right to a private life - was specifically mentioned in Recital 10 of the Directive as underpinning the level of protection for individuals outlined in the Directive[32]. The authors concluded by arguing for increased self-regulation in the form of organisational Data Protection Supervisors[33], combined with the provision of more information to the data subjects concerning the processing of their personal data. Crucial to the success of these recommendations was education, in particular, raising awareness among data subjects of their rights under the DPA 1998.

In other EU member states, industry specific codes of practice have attracted increased attention. The growth of the internet, and increased dissemination of personal data, point up to the increasing difficulty of regulating the flow of

personal data through 'one size fits all' national and transnational legislation. In the Netherlands, van de Donk and van Duivenboden[34] outlined the role of such codes in the national data protection system, where codes had been drawn up in consultation with the Dutch data protection authority. This form of 'controlled self-regulation' eased some of the pressure of enforcement from the national regulators, whilst allowing sectors of industry a degree of (officially approved) independence from the state - providing compliance was achieved with the codes. In the UK, codes of practice have been developed for the use of closed circuit television (CCTV)[35] and more controversially concerning employment practices[36].

The case for codes of practice has been strengthened by Article 25 (2) of the Data Protection Directive, allowing them to be taken into consideration when assessing the 'adequacy' of data protection in third countries. The academic lawyer, Shaffer[37] argued that the Directive has changed the way all US institutions addressed data protection issues. Since the enactment of the Directive, US businesses have been prodded to change their behaviour in order to avoid confrontations with EU regulators; US regulators have pressed US businesses to enhance their internal standards to avoid a regulatory conflict; and US privacy advocates have been presented with a functioning alternative to US law which they can promote. This analysis implied that the personal data of EU member states should be secure when transferred to the US in accordance with the 'Safe Harbor' agreement reached in July 2000[38]. Long and Quek[39] concurred, assessing the 'Safe Harbor' agreement in the context of the debate over the impact of globalisation on state sovereignty. Writing in 2001 (published 2002) the authors argued that the actions of the US illustrated the degree to which even a powerful state has had to make substantial changes in its policies and, to a lesser extent, its institutions due to the external forces of globalisation.

Raab, one of the most prominent researchers in data protection over the last decade, has published detailed articles focusing on the relationships *within* the various national data protection models – involving people, roles and institutions. In 1997, he argued that, if privacy was to be safeguarded, it would become increasingly important to comprehend – even shape – the connections among the various mechanisms or strategies, and among those who deploy them[40]. Raab

advocated a position in which the various market, civil society and state forces involved in 'co-producing' effective data protection were mutually dependent. However, this approach required further detailed empirical and comparative investigation across systems in order for privacy and data protection to emerge as a coherent field of public policy.

Bennett and Grant considered four possible futures for data protection in the excellent *Visions of Privacy*[41] – a collection of essays by prominent academics and campaigners in the field. The first was the surveillance society, in which the individual would have little or no control over the collection and circulation of personal information. The second scenario comprised an incoherent and fragmented patchwork of data protection, where the pressures for surveillance would continue, but would be punctured by periodic and unpredictable victories for the privacy value. A third vision, perhaps the one currently in existence, was of privacy haves and have-nots. Some societies would apply instruments for data protection comprehensively and vigorously. Others, like the US, would react to privacy issues as they emerged in particular sectors. Finally, an optimistic vision was put forward of global privacy standards, with instruments of privacy protection spreading as a process of 'ratcheting up' to the standard of the EU Data Protection Directive. The authors correctly concluded that any of the above futures was possible, and could result from an explicit policy choice – by organisations applying data protection principles and building privacy into their practices, and by individuals protesting surveillance out.

### 3.1.4 Sources of information on data protection

#### *Standard legal texts*

Several standard books – aimed at practitioners - explain the content of the DPA 1998. For detailed line-by-line analysis of the Act, together with a copy of the statute, Carey's *Data protection in the UK* proved a very useful reference source[42]. It is a comprehensive guide - assuming no prior knowledge of data protection legislation. The book is structured logically, with chapters on the rights of

individuals, the data protection principles, exemptions and enforcement. In addition, specific chapters are dedicated to the internet, telecommunications and the obligations of employers.

A more critical text is Jay and Hamilton *Data Protection: law and practice*[43]. Comprehensive like Carey, Jay and Hamilton, however, attempt greater historical detail: making greater reference to case law and to a series of hypothetical cases. The authors highlighted the limitations placed on the DPA 1998 - particularly its failure to address privacy, in spite of the clear provisions in the overarching EU Data Protection Directive relating to private life. This, argued the authors, could lead to problems in UK courts with lawyers arguing that the Directive has not been fully transposed into UK law[44]. On the HRA 1998, the authors made the important point that the manner in which the Convention has been inserted into UK law did not endow individuals with a direct right to take action in courts for breach of their privacy. The right must be respected by the state, but if an individual's privacy is breached by a private party, the litigant has no basis on which to take action in breach of that right alone[45]. However, not all commentators agree with this interpretation. The views of Singh, a human rights barrister, will be considered in section 3.2 of this literature review. Nevertheless, Jay and Hamilton helped highlight such procedural complexities. In addition, they clarified what was missing from the DPA 1998, what needed to be developed through case law (for example the nature of the right to private life), and included a detailed case study on the definition of 'relevant filing system'. A privacy culture based on both the DPA 1998 and the HRA 1998 may be possible, but it will take many years as it will need to be established via the UK courts.

*Academic journals*

The enactment of the Data Protection Directive in 1995 dramatically increased privacy research across many disciplines – including law, social sciences and politics. As a forum for detailed analysis of such research, the academic journals proved most enlightening. For instant analysis, electronic journals have been particularly useful – combining academic articles with more descriptive commentaries. Publications include *The Journal of Law, Information and*

*Technology (JILT)*[46] based at Warwick Law School, Warwick University and the *Web Journal of Current Legal Issues*[47] published bi-monthly at Newcastle University. The former has been especially prolific, with a dedicated data protection issue in January 1996[48] featuring articles outlining the European Directive - from the introduction by Lloyd[49] to features on its impact in various European countries such as Denmark, UK, Ireland and the Netherlands. Recent issues have considered technologies for privacy protection[50].

The *Web Journal of Current Legal Issues (WJCLI)* is less orientated towards the information sector, but has featured some comment on data protection. Kosten and Pounder provide a detailed Article-by-Article analysis of the Data Protection Directive, drawing attention to some of the difficulties that may occur during the implementation of the Directive into UK law[51]. Difficulties included exemptions 'in the public interest'[52] - exemptions balancing right to privacy with 'rules governing freedom of expression'[53] which could be problematic, possibly conflicting with Article 10 of the ECHR. Further detail can be found with Widdison's article which tabulated the key changes between the 1984 and 1998 Data Protection Acts[54]. More recent editions of *WJCLI* have featured freedom of information considerations[55] and the privacy implications of recent legislation permitting greater inception of communications by public organisations and business[56].

In terms of ongoing research, the hard copy journals proved an excellent source of information, for example: *International Review of Administrative Sciences*; *Cambridge Law Journal*; *Journal of Common Market Studies*; *The Information Society*; *Information, Communication and Society*; *European Human Rights Law Review*; *Science, Technology and Human Values*. Finally, the *International Review of Law, Computers and Technology* dedicated issues one and two to data protection in 1997, whilst in 1999 *Revue Français d'Administration Publique* featured a special issue (number 89) concerning the transposition of the EU Data Protection Directive into several counties. The above journals are generally more geared towards refereed articles than commentaries, often showcasing research conducted over a number of years. This included studies into the effectiveness of the DPA 1998, development of a methodology for assessing the workability of

data protection legislation, comparison of data protection law cross-nationally, and questions concerning the causes and effects of surveillance. Naturally, the journals in this subsection represent a sample of the publications in existence. In particular, there are many other relevant law journals, especially in the US.

*Newsletters*

Business newsletters are essential for providing expert opinion on new developments within organisations – often prior to the publication of academic research in the area concerned. *Privacy Laws and Business* are a consultancy firm, producing international and UK newsletters concerning the impact of data protection law on the public and private sectors. A recent issue of the international newsletter featured activities of the European Commission during autumn 2002[57]. Particular attention was given to possible amendments to the Data Protection Directive, and to consultation concerning a proposed directive on workers' personal data. The UK edition has highlighted strategies employed by various organisations to achieve compliance with the DPA 1998 including retailers[58], banks[59], and health[60].

The style and structure of the newsletters varies considerably. *Privacy and Data Protection*, edited by Carey, was established in 2000 and dedicated largely to UK data protection issues, such as the debate over the use of the electoral roll for marketing purposes[61] and how employers cope with subject access requests from employees[62]. It has featured perspectives from overseas – with regular views from the US in particular. Finally, the journal provides an information service for subscribers – allowing receipt of documents free of charge.

In the US, the monthly *Privacy Journal* tackles 'privacy in the computer age'. At approximately eight pages in length, it is lighter than the newsletters mentioned above. Additionally, it does not feature contributions from external commentators – being more of a news digest of privacy issues in the US. The only outside contributions – sometimes from privacy experts – come in the letters page. As a result, the journal, although a useful source of information, has a narrower perspective compared with some newsletters.

There is also a body of electronic newsletters. They tend to be less substantial in content, usually structured as news digests. *Act Now* details data protection issues in the UK public sector. In addition to news stories, it lists details of relevant conferences and other resources such as guides to the DPA 1998 by government departments, and training seminars on the Act. In the US, the Electronic Privacy Information Center (EPIC), a civil liberties group and research centre, publishes the bi-weekly *EPIC Alert*[63]. This is a well ordered subscription newsletter, with a table of contents outlining the articles featured, a bookstore cataloguing other publications, and a list of conferences. Additionally, the 'EPIC Bill-Track' feature charts the progress of privacy-related legislation through Congress. Altogether, this newsletter provides a clear, informative picture of current US privacy policy and debate. Another prominent electronic newsletter, and forum for discussion of the effect of technology on privacy, is the *Computer Privacy Digest*[64].

Other newsletters include: in the UK, *Data Protection and Privacy Practice*; in the US, *Privacy Times* and *Privacy and American Business*; in Canada, *Privacy Files*; and in Australia, *Privacy Law and Policy Reporter*. Finally, solicitors such as Masons[65] and Bird and Bird[66] produce their own newsletters detailing recent legal developments in privacy law.

### 3.1.5 The wider debate

#### *Government*

The official source for information concerning data protection policy and implementation in the UK is the OIC. In her *Annual Report* for 2002[67], the Commissioner looked forward to the challenges faced by the government's response to terrorism and to freedom of information. Other pressing issues included public registers, particularly the use of the electoral roll, and reviewing the OIC's current enforcement powers. The Commissioner's *Annual Reports* are thus key documents outlining what the supervisory authority view as significant issues, and priorities for the subsequent 12 months. Finally, appendices to the

2002 *Annual Report* detail various statistics and performance indicators regarding notifications processed, complaints investigated, customer and level of public awareness.

Within the European Union, data protection largely falls under the remit of the Data Protection Unit at the Internal Market Directorate. This Directorate's website has access to a variety of resources[68]. They include news, working papers, and studies into data protection, in addition to other international instruments on the topic, for example Convention 108[69]. Convention 108 had been drafted by the Council of Europe[70], and opened up for signature in 1981 as world's first legally binding international data protection measure, setting a precedent for the 1995 EU Data Protection Directive[71].

*Non Government Organisations (NGOs)*

Civil liberties groups have become increasingly influential in lobbying government for changes to the law, often commissioning their own studies into key aspects of privacy. Considerable information is included on their websites: Cyber-Rights and Cyber-Liberties (http://www.cyber-rights.org) containing detailed information on RIPA; the Foundation for Information Policy Research (http://www.fipr.org), also heavily involved in the RIPA issue; Campaign for Freedom of Information (CFOI) (http://www.cfoi.org.uk) lobbying the government for changes to the freedom of information legislation; and Liberty (http://www.liberty-human-rights.org.uk) which has reported across a range of issues concerning human rights. The above sources have been complemented by the websites of pressure groups such as Statewatch (http://www.statewatch.org), monitoring state and civil liberties in the EU, and the aforementioned civil liberties organisation EPIC (http://www.epic.org).

The identification and availability of reports by such interest groups can be difficult. A key source for such documents has been expert privacy websites such as Privacy Exchange, (http://www.privacyexchange.org), and Privacy International, (http://www.privacy.org/pi/). The former website has an informative section listing reports in the field including those by governments and

civil liberties organisations. In 2002, separate reports were published by the US government and EPIC concerning privacy and consumer issues[72].

Finally, a key report was commissioned by Privacy International and the US-based civil liberties group, EPIC. *Privacy and Human Rights 2002*, reviewed the state of privacy in over fifty countries[73]. It examined the impact of government anti-terrorism measures following the attacks of 11 September 2001. Trends identified included increased communications surveillance, and further profiling and identification of individuals. Conversely, the report discovered that laws to protect privacy in the workplace are gathering more support, and efforts to enact new data protection laws continue in Eastern Europe, Asia and South America. Thus, there is an active campaigning community regarding privacy interests.

*Expert forums*

Expert discussion forums play an important role in shaping the debate on data protection and privacy. The Data Protection Forum is a discussion group bringing together companies, public sector and consumers to discuss personal data in seminars. Presentations have been by organisations as diverse as the National Consumer Council and Deloitte, Touche. During 2002, seminars have been held on subject access requests, data protection in the workplace and international data sharing. Many of the presentations are available to members at: http://www.dpforum.org.uk/previous.shtml.

The JISCmail-hosted *Data Protection Discussion Group*[74] helps to promote the discussion of data protection among UK lawyers, academics and data protection officers. Online discussions include how the Act will work with regard to workplace surveillance, sensitive data – such as student names held by universities - and genetic data. The relevance of the discussions, and the standard of the inputs, is inevitably varied. Yet, it generally represents a worthwhile contribution to the debate on data protection.

*Consumer opinion*

Important raw data can be gathered from surveys. This subsection details a sample from the US and Europe. Privacy Exchange has a detailed list of privacy surveys dating from 1979[75]. Among the most prominent is the long series of surveys Equifax/Harris have undertaken since 1979 - under the direction of Alan Westin and heavily funded by industry, in particular the Equifax credit rating service. One of the most recent in the series followed the terrorist attacks in New York on 11 September 2001[76]. This survey found customers demanding that companies increase measures to protect handling of their personal data, with 84% of respondents believing that company privacy policies should be independently verified. Key concerns regarding handling of personal information included: providing information to third parties without permission (75%) and lack of security (70%). Another US survey is by the Pew Internet and American Life Project who have published reports on various topics, for example: September 11 and the internet – one year on (2002); e-government (2002); and fear of online crime (2001)[77].

Another valuable website for such information is http://www.nua.ie/surveys - an online information database - containing statistics on all aspects of the internet, including privacy. Usefully, the information is provided in order of date, complete with links. Examples include an October 2002 survey stating that the percentage of Americans using the internet more frequently was still increasing, although the level of trust had fallen, with only 21% of internet users believing that making purchases online was secure[78].

In the UK, annual surveys are conducted by the regulatory authority, the OIC, for fifteen years the Office of the Data Protection Registrar (ODPR). This information can be found on the OIC website http://www.dataprotection.gov.uk/dpr/dpdoc.nsf [79]. Commencing in 1987, public attitudes towards the use of personal data were tracked. Questions concerned attitudes towards personal privacy and the DPA – including awareness of the Act among data subjects. This had increased from 34% in 1987 to 71% in the 2001 survey, the most recent research available. Other UK surveys include Perri 6's

study *The future of privacy*[80] for the think-tank DEMOS. Among the findings were that few people saw any loss of privacy as inevitable, and that very few were willing to trust any organisation – with supermarkets found to be the least trusted, few people being convinced that their loyalty cards are treated with enough confidentiality.

Finally, Consumers International published *Privacy@net*[81] an international comparative study into consumer privacy on the internet in 2001. The research was conducted by an international project team, with participants from 14 consumer organisations around the world assessing the approach of 751 internet sites to data protection. Among the findings were that just over two thirds of sites collected some sort of personal information, and that the vast majority of websites gave users no choice about being on the site's mailing list or having their name passed onto affiliates or third parties. Perhaps one of the more surprising findings was that the most popular US sites were more likely than the EU ones to give users a choice about being on the company's mailing list or having their name passed on, despite the Data Protection Directive obliging EU member states to provide users with a choice[82]. The report concluded with a series of recommendations including the need for greater consumer control over collection, use and disclosure of their personal data and the establishment of an independent oversight body to ensure compliance. This important report received considerable publicity at the time of publication, plus invitations from legislators to discuss the findings. When asked in September 2001 whether they would be conducting any further investigations into data privacy, Consumers International answered: "Yes, we hope to but it depends on funding and won't be for 2-3 years."[83]

*Media debate*

One of the paramount ways of keeping up to date has been via the quality press. *The Guardian* in particular has produced regular and well-informed pages on information issues, as well as launching its own campaign for greater openness in government in the wake of the proposed freedom of information legislation[84]. Additional relevant articles have been found via newspaper databases such as British Newspaper Index and European Intelligence Wire[85]. Those references

have yielded commentary on the RIPA, as well as a variety of consumer issues such as online purchasing, CCTV and workplace surveillance.

*The Guardian* has recently featured stories concerning the UK governments' attempts to facilitate electronic government (or 'e-government)[86]. The expenditure of £1 billion to date has raised questions about its potential benefits. The online media is now an important source – allowing quick and easy access to breaking news. *FT.com* – the online arm of the *Financial Times* – was one of the many sites that broadcast the UK government's retreat during summer 2002 over the expansion of RIPA 2000[87]. Other stories featured recent EU legislation concerning junk emails, or spam[88], and the online *Independent* has discussed the rise of CCTV[89].

Further coverage of the debate on privacy is located on online business news services such as Silicon.com and CNET Networks. The latter mentioned attempts of pressure groups in the US to force the online retailer, Amazon, to tighten up its privacy policies[90]. Silicon, meanwhile, broke a story in May 2002 concerning the new Electronic Communications Directive[91], and attempts by some EU member states to allow retention of telecommunications traffic data for not just national security, but also for the prevention, investigation, detection and prosecution of criminal offences[92]. This has been strongly opposed by civil liberties groups as an unwarranted invasion of privacy.

For further international legal perspectives, the EU-based QuickLinks provides links to news items about the legal and regulatory aspects of the internet and the information society. The website http://www.qlinks.net contains frequent updates, an events page and news items organised by category (for example, 'Data Protection') as well as chronologically by issue and full text search. This source has proved to be the first point of reference for breaking news, providing citations that can be followed elsewhere.

## 3.2 Human Rights

The significance of the HRA 1998 was stressed in the quality press. On the day it came into force – 2 October 2000 - a front page caption on *The Guardian* read 'UK law sees the biggest change in more than 300 years'[93]. BBC Online ran a special feature during the first week of the Act, analysing its effect on the police, health, councils and workplace among other institutions[94]. Additionally, the Act has been warmly welcomed by the OIC, believing it will strengthen the application of the DPA 1998, as well as reinforcing the case for privacy and data protection more widely. An alternative journalistic view of the HRA 1998 came from Davies, who saw lawyers as the main beneficiaries from the spate of litigation that will stem from the Act[95].

### 3.2.1 Incorporation of European Convention of Human Rights

As the UK DPA 1998 is ultimately derived from the ECHR[96], especially Article 8, an initial understanding of human rights legislation is fundamental. Wadham and Mountfield's *Blackstone's guide to the Human Rights Act 1998* provided an excellent introduction to the HRA 1998[97]. The authors began by pointing out that the HRA 1998 only incorporated part of the ECHR. It did not incorporate any of the procedural rights of the Convention, nor the right to an effective remedy (Article 13), although regard will be made to case law developed by the European Court of Human Rights at Strasbourg. Wadham and Mountfield proceeded to list the limitations of the Act, including issues such as the rule of law and whether any state interference was necessary in a democratic society or proportionate to the ends achieved, for example, the protection of privacy from excessive media interference. Usefully, the authors examined each Convention right, and issues that could be raised in UK courts. For Article 8, important issues existed regarding police listening devices, CCTV and employee privacy. The book also has a valuable table of cases referred to in the text, and appendices concerning background policy papers, parliamentary debates, rules of procedure for the European Court of Human Rights and the text of the ECHR. Altogether, this is a fundamental reference source.

### 3.2.2 Privacy and human rights context

Specific academic research concerning privacy and human rights has been more difficult to locate. The information aspect of the right to privacy – data protection – has been analysed in detail in section 3.1. Research into the cultural context of privacy as a human right has been limited. In 1994, a wide-ranging study into the issues surrounding privacy and human rights in the international context was published by Michael as *Privacy and Human Rights*[98]. The author examined the social, political and cultural context to global privacy and data protection laws, highlighting the difficulties that the term 'privacy' may present to different societies and the diverse legal approaches taken to its protection.

The legal approaches were categorised under three headings: Nordic, civil and common. Nordic was defined as a combination of legal remedy available to the individual through rights of access and the administrative regulation of computerised records. In many ways, this form of remedy pioneered information legislation. Certainly, rights of access were well entrenched, with Sweden having a Freedom of the Press Act in 1776, the oldest such law in the world. Sweden also led the way in regulation of computerised records, with the world's first national data protection law in 1973[99].

The civil law approach differed in that it relied on statements of general principle. Its clear influence has been seen through the ECHR, a codification of international human rights law. Common law – the third approach identified by Michael - applied the principles through individual cases. In the UK, for example, the emphasis had been on particular legal remedies against particular infringements. Such rights were often developed by judges without reference to Parliament. An example would be the essentials of the English law of confidence. However, following the implementation of the first Data Protection Act in 1984, this trend had been somewhat eclipsed, with the UK establishing a supervisory body to police the legislation. Nevertheless, the enactment of the HRA 1998 has led to speculation that privacy common law may be developed. This issue will be

expounded later in Chapter 4. Michael concluded optimistically, stating that since the early 1970's the spread of automated information handling has almost been matched by the spread of legislation to protect individual privacy[100].

### 3.2.3 HRA 1998: recent research

Since the enactment of the HRA 1998 in October 2000, and the subsequent development of case law in this field, analysis in academic and legal journals has been increasing. This subsection comprises the writings of academics and practising lawyers concerning the possible development of a UK common law of privacy, based on the provisions of the HRA 1998.

One of the earlier analyses of the possibilities of the new legislation was by Singh. Writing shortly after the HRA had completed its passage through Parliament in autumn 1998, Singh presented a detailed interpretation of the right to privacy[101]. Although considering the interface between privacy and freedom of expression, his critique raised some interesting points in relation to privacy law. Firstly, Article 8 imposed an obligation to 'respect' privacy – not just prohibit interferences to privacy by the State. This distinction, Singh argued, is crucial as Strasbourg has stated the positive obligation will extend to requiring action to protect an individual from the acts of other private parties[102]. This could set a precedent, for example making employers accountable to the HRA 1998 in the private, as well as public, sector[103].

Secondly, Singh argued that a provision in the HRA 1998 – Section 6 (6) – preventing the possibility of a complaint being made that Parliament failed to legislate against a particular right, could lead judges to develop their own common law - extending far beyond the current breach of confidence case law. To summarise Singh's findings:

(i) The HRA 1998 may be indirectly applicable against private individuals and companies;

(ii) The HRA 1998 provided a springboard for developing existing causes of action, thus filling gaps in the patchy privacy protection provided in English law.

*Analysis of case law 2000-2003*

Academic and legal journals have analysed the privacy case law deriving from the HRA 1998 as and when judgements have been made. In this respect, the legal journals have been most prolific. Useful publications not previously mentioned in section 3.1.4 of this Chapter include: *New Law Journal*; *The Law Quarterly Review*; *European Law Review*; *Industrial Law Journal*; and *European Law Journal*. The standard of analysis varies from brief descriptions of a single case and its implications, to deeper analyses of the context to a number of judgements under the HRA 1998.

Elliot (2001)[104] was an example of the former – a brief report that analysed the *Douglas* case involving the celebrity wedding photographs[105]. Reviewing the summaries of the three judges, Elliot concluded that the judgement pointed to two important developments. Firstly, it corrected the long-standing failure of English law to embrace the right to privacy as a legal right capable of existing independently from that of the law of confidential information. Secondly, the ruling disclosed judicial unwillingness to isolate the development of English common law from the influence of Convention rights. Therefore, it conferred upon them a degree of 'horizontal effect' – that is, the rights applied to some extent to private individuals as well as public bodies. However, at the time of writing (January 2003) the case is still ongoing[106].

Singh and Strachan (2002)[107] took a longer view, placing the emerging law of privacy in historical context and considering how the English courts may secure privacy rights. The most recent cases reviewed were those involving supermodel Naomi Campbell's claim against the *Daily Mirror* for breach of privacy after being photographed leaving Narcotics Anonymous[108], and the footballer Gary Flitcroft's attempts to keep his extra-marital affairs out of the public domain[109]. In both cases, the judgements were reached in March 2002, although the Campbell

case is ongoing[110]. The authors argued that the HRA 1998 had become a catalyst for the development of the common law of breach of confidence. However, the courts although beginning to recognise the existence of a separate right to privacy, had yet to express that right in a clear and explicit way.

## 3.3 Individual privacy protection: the organisational dimension

### 3.3.1 New legislative framework: potential for conflict?

In the new legislative environment, perhaps the area where the impact of the new regulations is most uncertain is within organisations. In addition to the DPA 1998 and HRA 1998, the Department of Trade and Industry's (DTI's) *Lawful Business Practice Regulations*[111] and the OIC's *Draft Code of Practice: the use of personal data in employer/employee relationships*[112] have, or will have, a substantial bearing on workplace privacy. The Anti-Terrorism, Crime and Security Act (ATCSA) 2001[113] is also relevant. The above, and other legislation from 1988 onwards can be referred to via the HMSO website: http://www.hmso.gov.uk/acts.htm. Finally, official documents detailing reactions to government proposals are helpful, for example, in the case of the *Lawful Business Practice Regulations*[114].

In April 2002, the UK government addressed some of these concerns with the publication of its report *Privacy and data-sharing: the way forward for public services*[115]. A hugely significant document for all public organisations, *Privacy and data-sharing* sought to chart a course between achieving greater electronic provision of public services and the evolving legal framework concerning human rights issues and privacy. In order to achieve this, the public needed to trust the government with its personal data. To this end, 25 recommendations are made for public organisations, including: development of data standards to improve accuracy of personal data; adoption of the BS 7799 standard promoting information security; and the appointment of board level Chief Knowledge Officers to integrate issues such as data protection, human rights, freedom of information and records management. All public sector organisations are expected

to embody their service-level privacy agreements in a 'Public Service Trust Charter'. The 'Charter' is currently in the second round of consultation, with a view to being finalised by spring 2003[116].

Significant EU grey literature included the COM series of documents. These documents include proposals for legislation, annual reports, and policy statements. They can be traced via the excellent Eurolaw service at http://www.ili.co.uk. This site also includes Court case decisions and parliamentary questions. Finally, in order to focus on a particular piece of legislation for example, the Data Protection Directive, the European Parliament website <http://www.europarl.eu.int> has a helpful legal observatory with details on documents produced, the agents involved and providing commentary – mainly in French - on the various stages leading to the final text. This is an excellent facility and the first point of reference for any document search regarding EU legislation.

### 3.3.2 Academic and legal research

Extensive research into the practice of surveillance has been conducted over a number of years. In 1988 Clarke[117] used the term 'dataveillance' in a paper to describe the systematic monitoring of people's actions or communications through the application of information technology. The effects of this monitoring by public organisations, and attempts to limit it, have been studied by authors such as Westin, Miller, Rule and Flaherty – all mentioned in section 3.1. Important research in private sector activity in this field has been conducted by Cate[118] – advocating minimal legal and government intervention in the data handling practices of private organisations – and Reidenberg[119] - arguing for globalised standards for fair information practice, 'co-regulating' the divergent data protection practices of the EU and the US.

Surveillance within organisations has been discussed at length by Mohammed in a *JILT* article in 1999[120]. In a 1999 conference paper, Davies provided a detailed overview of the new technologies coming to the fore[121] – extending to every aspect of a worker's life. Miniature cameras monitor behaviour. 'Smart'

identification badges - popular with IT companies such as Olivetti Research in Cambridge - track an employee's movement around a building. Telephone Management Systems analyse the pattern of telephone use and the destination of calls. Computer-based monitoring systems record statistics about the employee assigned to a particular terminal, including the number of keystrokes per minute and the amount of time spent on the computer. Software such as Baltimore's MAILsweeper and WEBsweeper can monitor employee email and web use – blocking access to 'backdoor' email accounts such as Hotmail[122]. Finally, psychological tests, aptitude tests, performance tests, and personality tests – many of which are electronically assessed – raise a great many issues of privacy, control and fairness. For many employees, surveillance and monitoring have become part of the modern work environment.

Since the terrorist attacks of 11 September 2001, the privacy implications of anti-terrorism measures enacted by most Western governments have come under scrutiny. Malcolm and Barker (2002)[123] assessed the problems faced by communications providers – for example, telephone companies and internet service providers - in complying with the provisions of the UKs ATCSA 2001. Under the provisions of this Act, traffic data must be retained by organisations. Initially, this will be on a voluntary, self-regulating basis[124]. However, the possibility has been left open for compliance through statutory instrument[125]. The authors highlighted concerns about the compatibility of this provision with Principle Five of the DPA 1998 which stated that data must not be held any longer than necessary[126]. Moreover, the costs of compliance incurred by communications providers are likely to be significant[127]. New systems will have to be put in place to cope with increased demand for retention and access – by national security and law enforcement agencies, and by data subjects themselves - under the DPA 1998. As the EU was approving a new Directive in this field[128], the authors expected the UK government to enact the statutory option, compelling communications provides to retain such traffic data.

### 3.3.3 Regulating employee personal data

From the literature reviewed in this section, there is a requirement for organisations to devise clear policies concerning data collection, use and retention. Research into such policies forms a significant part of the case study fieldwork, the findings of which are discussed in Chapter 7. In particular, the way organisations process data belonging to their employees has been viewed by some regulators and academics as requiring further clarification. Given that data protection legislation generally governs the processing of *all* personal data – belonging to both clients and employees - held by organisations, the case for further legislation is contentious. Nevertheless, the European Commission has recently expressed its intention to legislate to safeguard workers' personal data, citing globalisation, technological advance and 'post 11 September insecurity' as the main drivers[129]. This proposal, and the response of employers in particular, is discussed in further detail in Chapter 6.

A detailed policy statement on the regulation on protection of employees' personal data was drawn up by academic, lawyer and former data protection regulator, Simitis in 1999[130]. The author believed that employees needed to be empowered to protect their own privacy. This is the reverse of current situation where the onus appears to be on employees, and the community at large, to show that surveillance is not necessary. Simitis defined eight areas – closely linked to the DPA 1998's eight data protection principles – as being crucial to the regulation of employee data. Chief among these, were the method of data collection, with informed consent of the employee being crucial, and the collective rights of the employees.

In many ways, the last factor summarised Simitis' point: that employees, collectively through representatives, should at least be informed and consulted prior to the introduction or modification of automated data processing systems; before direct and indirect electronic monitoring; and as to the purpose, content and prospective uses of any questionnaires or tests. However, it is highly unlikely that organisations, particularly in the UK, would accept such an increase in regulations. The course that the UK government has chosen to regulate employees privacy is

altogether more moderate, as demonstrated by the *Lawful Business Practice Regulations 2000*. This measure actually legally permits employers to read staff emails and monitor websites visited by staff - if they *think* an employee is committing a crime or doing something 'unauthorised'[131].

At the same time, the OIC's recent draft *Code of Practice* in this area is almost certainly relevant to monitoring of personal electronic communications such as email. According to the draft *Code*, employers have to ensure that monitoring is in such a way that it does not intrude unnecessarily, otherwise employers who acquire information under the *Lawful Business Practice Regulations* could still be prosecuted by the OIC. The employer clearly needs a system that complies with three Acts – the DPA 1998, HRA 1998 and RIPA 2000 - so the one most favourable to employees will determine how much employers can intercept. Currently, the DPA's *Draft Code of Practice* offers most protection. However, according to the OIC, this *Code* is now not due to be finalised until "Easter 2003"[132].

## 3.4 Conclusions

From this literature review, three strands of the debate can be identified that are of particular interest to this study:

(i) The increasing difficulty of regulating the flow of personal information through the 'one size fits all' national and transnational legislation that has been favoured by European nations for three decades.

The difficulty of defining information privacy ensured that safeguarding individual rights in this field has been a formidable task from the outset. With the increased dissemination of personal data via stand-alone computers rather than centralised government databanks, data protection law needs to evolve. Sector-specific codes of practice and model agreements (such as 'Safe Harbor') between organisations

trading in different countries have become increasingly prevalent, with privacy being viewed as a quality standard to be 'built-in' to good business practice.

(ii) The possible development - in the absence of privacy legislation - of privacy common law by the UK courts.

The method of incorporating the ECHR into UK law devised by the government has ensured that the HRA guarantees the right to privacy. However, an individual cannot take action in breach of that right alone. The rulings in the *Douglas* and *Campbell* suggested that, although the HRA 1998 is still in its infancy and both cases are still in progress, a separate privacy common law remains a distinct possibility.

(iii) The regulatory morass regarding privacy in organisations.

In particular, the relationship between the *Lawful Business Practice Regulations* and the *Draft Code of Practice: The use of personal data in employer/employee relationships* has caused confusion. The OIC believe that the two can work in tandem, but trade unions and employers' organisations remain to be convinced[133]. The ATCSA 2001 has added to the uncertainty, particularly for communications providers. The government report *Privacy and data-sharing* outlined important recommendations that will have a significant impact on the handling of personal data in the public sector, aiming to streamline procedures and build trust between individuals and the state. Finally, organisations have been increasingly devising their own privacy standards - based on official guidance, but shaped around their particular corporate needs. Organisational privacy policies have been studied as part of the case study fieldwork, discussed in Chapter 7.

There is certainly a flourishing and vibrant debate in this field - with contributions from civil liberties organisations, the quality press, academics and discussion

groups. Various fora for exchanging ideas exist - providing important stimuli for the future development of data protection policy research.

Comparative studies have increased the knowledge of experience overseas. Indeed, the EU Data Protection Directive can be viewed as a testament to incorporation of some of the diverse legislative strands identified by Bennett - particularly the ombudsman approach from Germany, and the promotion of sector specific codes of practice prominent in the Netherlands. There is considerable uncertainty as to whether recent UK legislation offers adequate protection for individual's personal data. Both the DPA 1998 and the HRA 1998 are relatively recent Acts of Parliament, with little case law to date. Consequently, the bulk of the literature concerning the legislations' impact on organisations has been necessarily speculative. Thus, there is a need for a detailed critical study of this nature into the effect of the DPA 1998 on the data handling processes of public organisations. Such research will be required to develop the findings of the academics and lawyers referred to in this literature review.

## References and Notes


[1] European Communities. Commission. *Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.* Official Journal of the European Communities. No. L281/31 (23/11/95).

[2] Great Britain. *Data Protection Act 1998.* London: HMSO.

[3] Council of Europe. *Convention for the protection of human rights and fundamental freedoms.* Strasbourg 1950.

[4] Great Britain. *Human Rights Act 1998.* London: HMSO.

[5] Miller, A. *The assault on privacy*, 1971, p.169.

[6] Westin, A.F. *Privacy and freedom*, 1967.

[7] Miller, A., ref. 5.

[8] Westin, A.F., ref. 6, p.7.

[9] Miller, A. ref. 5, p. 25.

[10] Rule, J.B. *Private lives and public surveillance*, 1973.

[11] The European Community became the European Union when a revised European Treaty (agreed at Maastricht) came into force in November 1993.

[12] Burkert, H. Institutions of data protection: an attempt at a functional explanation of European national data protection laws. *Computer Law Journal,* 1982, 3 (2), 167-188.

[13] *Ibid.*, pp. 180-1. The author cites examples of educating the general public through 'participating in forums, producing brochures, and by making media appearances'. Data users (known under the 1995 Data Protection Directive as 'data controllers') can be educated through user guides or manuals; data subjects can be given advice in specific cases; and data protection authorities advise legislators, therefore participating in making information policy.

[14] *Ibid.*, p.184. That is, the powers involving the executive, legislature and judiciary.

[15] *Ibid.*, p.188.

[16] Nugter, A.C.M. *Transborder flow of personal data within the EC*, 1990. The countries analysed were West Germany, the Netherlands, France and the UK.

[17] *Ibid.*, pp.317-321.

[18] Refer to Chapter 4 for further discussion of this process.

[19] Flaherty, D. *Protecting privacy in surveillance societies*, 1989. The author studied data protection and privacy laws in West Germany, Sweden, France, Canada and the United States.

[20] The United States was the only country Flaherty studied that did not – and still does not – have any sort of supervisory authority overseeing compliance with its privacy and data protection legislation.

[21] Flaherty, D. ref. 19, pp. 371-407.

[22] Bennett, C.J. *Regulating privacy: data protection and public policy in Europe and the United States*, 1992.

[23] Refer, for example:

- Bennett, C.J. Regulating the computer: comparing policy instruments in Europe and the US. *European Journal of Political Research*, 1988, 16 (5), 437-466.

[24] *Ibid.* pp.441-444.

[25] For example, refer:

- Kosten, F. and C. Pounder. The EC Data Protection Directive 1995: An analysis. *Web Journal of Current Legal Issues* [online], 1996 (2). (URL: http://webjcli.ncl.ac.uk/1996/issue2/kosten2.html) [Accessed 16/01/03].

[26] Pearce, G. and N. Platten. Achieving personal Data Protection in the European Union. *Journal of Common Market Studies*, 1998, 36 (4), 529-547.

[27] Bainbridge, D. and G. Pearce. Tilting at windmills – has the new Data Protection law failed to make a significant contribution to rights of privacy? *The Journal of Information, Law and Technology* [online], 2000 (2). (URL: http://elj.warwick.ac.uk/jilt/00-2/bainbridge.html) [Accessed 16/01/03].

[28] To quote a recent example: in the case involving Naomi Campbell being photographed outside Narcotics Anonymous, the *Daily Mirror*, on being found guilty of breaching the DPA 1998 was fined just £3500. Refer:

- Hall, S. and C. Dyer. Legal landmark as Naomi Campbell wins privacy case. *The Guardian*, 28/03/02. (URL: http://media.guardian.co.uk/news/story/0,7541,675295,00.html) [Accessed 16/01/03].

However, this verdict was overturned on 14 October 2002. Refer:

- BBC News Online. Mirror wins Campbell appeal. *BBC News Online.* 14/10/02. (URL: http://news.bbc.co.uk/1/hi/uk/2327385.stm) [Accessed 16/01/03].

[29] Bainbridge, D. and G. Pearce, ref 27, section 2.2.

[30] The conditions for processing personal data under the DPA 1998 are set out in the Schedules at the end of the Act. The conditions vary according to whether the data is sensitive, or not, and also differ for data being transferred outside the EEA. Conditions other than consent include processing for: the legitimate interests of the data controller (Sch. 2, 6 (1)); performing any legal right or obligation in connection with employment (Sch 3, 2 (1) regarding sensitive data); the performance of a contract between the data subject and data controller (Sch 4, 2(a) regarding transfers to third countries).

[31] Bainbridge, D. and G. Pearce, ref. 27, section 3.4.

[32] *Ibid.*, section 4.

[33] The power to make this provision, central to data protection law in Germany, exists under section 23 of the UK DPA 1998. However, this power has not been exercised by the Secretary of State, and is unlikely to be used in the near future.

[34] Van de Donk, W.B.H.J. and H.P.M. van Duivenboden. Privacy as a policy: policy implementation perspective on data protection at shopfloor level in the Netherlands. *International Review of Administrative Sciences*, 1996, 62 (4), 513-534.

[35] Great Britain. Office of the Data Protection Commissioner. *CCTV Code of Practice*, 2000.

[36] Great Britain. Office of the Data Protection Commissioner. *Draft Code of Practice: The use of personal data in employer/employee relationships.* 2000. Parts of this Code are still (January 2003) in the process of being drafted. For further detail, refer to Chapter 4.

[37] Shaffer, G. Globalization and social protection: the impact of EU and international rules in the ratcheting up of US privacy standards. *Yale Journal of International Law*, 2000, 25 (1), 1-88.

[38] 'Safe Harbor' refers to the set of principles the US negotiated with the EU for US companies to voluntarily sign up to. The principles provide a 'Safe Harbor' for US companies to continue to trade with the EU.

[39] Long, W.J. and M.P. Quek. Personal data privacy protection in an age of globalisation: the US-EU safe harbor compromise. *Journal of European Public Policy*, 2002, 9(3), 325-344.

[40] Raab, C.D. Co-producing data protection. *International Review of Law Computers and Technology*, 1997, 11 (1), 11-24.

[41] Bennett, C.J. and R. Grant. Conclusion. *In*: C.J. Bennett and R. Grant (eds). *Visions of Privacy: policy choices for the digital age*, 1999, pp. 263-7.

[42] Carey, P. *Data protection in the UK*, 2000.

[43] Jay, R. and A. Hamilton. *Data Protection: law and practice*, 1999. Other comprehensive guides to the DPA 1998 include:

- Singleton, S. *Data Protection: the new law*, 1998;
- Lloyd, I. *A guide to the Data Protection Act 1998*, 1998.

[44] The European Court of Justice has developed the 'doctrine of direct effect' as a tool to employ when Member States fail to implement a Directive properly. This allows individuals to rely directly on the terms of the Directive rather than national law in these cases. However, this can only be relied on against organisations treated as part of the state, not the private sector.

[45] Jay, R. and A. Hamilton. ref 43, p.18.

[46] *The Journal of Information, Law and Technology* [online]. (URL: http://elj.warwick.ac.uk/jilt) [Accessed 16/01/03].

[47] *The Web Journal of Current Legal Issues* [online]. (URL: http://webjcli.ncl.ac.uk) [Accessed 16/01/03].

[48] For contents page of the Data Protection Issue refer:

- *The Journal of Information, Law and Technology* [online], 1996, 1. (URL: http://elj.warwick.ac.uk/jilt/issue1/1DP.htm) [Accessed 16/01/03].

[49] Lloyd, I. Introduction to Data Protection Directive: special feature. *The Journal of Information, Law and Technology* [online], 1996, 1. (URL: http://elj.warwick.ac.uk/jilt/dp/introd.htm) [Accessed 16/01/03].

[50] Refer:

- Borking, J. and C. Raab. Laws, PETs and Other Technologies for Privacy Protection, *The Journal of Information, Law and Technology* [online], 2001, 1. (URL: http://elj.warwick.ac.uk/jilt/01-1/borking.html) [Accessed 16/01/03].
- Kenny, S. and J. Borking. The Value of Privacy Engineering, *The Journal of Information, Law and Technology* [online], 2002, 1. (URL: http://elj.warwick.ac.uk/jilt/02-1/kenny.html) [Accessed 16/01/03].

[51] Kosten, F. and C. Pounder. ref., 25.

[52] *Directive 95/46/EC*, ref. 1, Article 7 (e).

[53] *Ibid.*, Article 9.

[54] Widdison, R. Data protection law: the key changes. *Web Journal of Current Legal Issues* [online], 1998, (4). (URL: http://webjcli.ncl.ac.uk/1998/issue4/widdis4.html) [Accessed 16/01/03].

Again, UK data protection law is discussed in further detail in Chapter 4.

[55] Cornford, T. The Freedom of Information Act 2000: genuine or sham? *Web Journal of Current Legal Issues* [online], 2001 (3). (URL: http://webjcli.ncl.ac.uk/2001/issue3/cornford3.html) [Accessed 16/01/03].

[56] Best, K. and R. McCusker. The scrutiny of the electronic communications of businesses: striking the balance between the power to intercept and the right to privacy? *Web Journal of Current Legal Issues* [online], 2002 (1). (URL: http://webjcli.ncl.ac.uk/2002/issue1/kb-rm1.html) [Accessed 16/01/03].

[57] Refer:

- Privacy Laws and Business. EU DP Directive review. *Privacy Laws and Business (International)*, 2002, 65, 6-8;
- Privacy Laws and Business. EU directive on workers' data. *Privacy Laws and Business (International)*, 2002, 65, 13-14.

[58] Privacy Laws and Business. Marks and Spencer – raising staff awareness. *Privacy Laws and Business (UK)*, 2002, 7, 6-8.

[59] Privacy Laws and Business. How Barclays human resources is implementing the new Data Protection Act. *Privacy Laws and Business (UK)*, 2001, 4, 10-12.

[60] Privacy Laws and Business. How the London Clinic piloted the DPA Audit Manual. *Privacy Laws and Business (UK)*, 2001, 4, 19-21.

[61] Privacy and Data Protection. New regulations on electoral role data spell doom for marketers. *Privacy and Data Protection*, 2002, 2 (6), 1, 13.

[62] Hurley, N. Employers' duty of disclosure following a data subject access request. *Privacy and Data Protection.* 2002, 2 (5), 6-8.

[63] For subscription details, refer URL: http://www.epic.org/alert/ [Accessed 16/01/03].

[64] For further details, refer URL: http://www.uwm.edu/Org/comp-privacy/ [Accessed 16/01/03].

[65] Masons publish a quarterly newsletter *Data Protection and Privacy Practice.* For subscription details, refer URL: http://www.masons.com/php/page.php3?page_id=dataprote8870 [Accessed 16/01/03].

[66] Bird and Bird publish newsletters on various issues relevant to this paper – including employment and IT law. For further details, and sample back issues, see URL: http://www.twobirds.com/NewsAndPublications/NewsLetters/newsletters.cfm [Accessed 16/01/03].

[67] Great Britain. Office of the Information Commissioner. *Annual Report and Accounts for the year ending 31 March 2002*, 2002.

[68] Refer to Data Protection Unit, Internal Market Directorate General, European Commission. URL: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm [Accessed 16/01/03].

[69] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, ETS no. 108. Strasbourg, 1981.

[70] The Council of Europe is an inter-governmental organisation that was set up in 1948 to help unite Europe after the Second World War. Distinct from the EU, the Council of Europe aimed to protect human rights - being responsible for the European Convention of Human Rights and administering the European Court of Human Rights. For further details, refer to URL: http://www.coe.int [Accessed 16/01/03].

[71] The UK signed Convention 108 in May 1981, and enacted the Data Protection Act 1984 in order to ratify the Convention. By 1990 – when the Commission first drafted a general data protection directive - the number of ratifications of Convention 108 had risen to ten.

[72] Refer:

- United States. Federal Trade Commission. *Public workshop: the mobile wireless web, data services and beyond: emerging technologies and consumer issues*, 2002;
- Gellman, Robert. *Privacy, consumers and costs: how the lack of privacy costs consumers and why business studies of privacy costs are biased and incomplete*, 2002.

[73] EPIC and Privacy International. *Privacy and Human Rights 2002*, 2002. (URL: http://www.privacyinternational.org/survey/phr2002) [Accessed 16/01/03].

[74] To join this academic discussion group, refer URL: http://www.jiscmail.ac.uk/lists/data-protection.html [Accessed 16/01/03].

[75] Refer to URL: http://www.privacyexchange.org/iss/surveys/surveys.html [Accessed 16/01/03].

[76] Harris Interactive and A. F. Westin. First major post-9/11 finds consumers demanding customers do more to protect privacy. *Harris Interactive* [online], 20/02/02. (URL: http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429) [Accessed 16/01/03].

[77] For list of Pew Internet reports, refer to URL: http://www.pewinternet.org/reports/ [Accessed 16/01/03].

[78] Nua surveys. More Americans online, but trust still an issue. *Nua.com*, 17/10/02. (URL: http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905358466&rel=true) [Accessed 16/01/03].

[79] For survey data, refer to 'Annual Reports'; then 'Media Briefing Microsite'.

[80] 6, P. *The future of privacy: volumes 1 and 2*, 1998.

[81] Consumers International. *Privacy@net: an international comparative study of privacy on the internet*, 2001. (URL: http://www.consumersinternational.org/) (Search under 'Publications'). [Accessed 16/01/03].

[82] *Directive 95/46/EC*, ref. 1, Article 14 (b).

[83] Interview with Naja Felter, Consumers International, London. 25/10/01.

[84] For details, refer URL: http://www.guardian.co.uk/freedom/ [Accessed 16/01/03].

[85] Both databases are available at Loughborough University's Pilkington Library on networked CD-ROM.

[86] Cross, M. Is e-gov worth it. *The Guardian*, 09/01/03. (URL: http://www.guardian.co.uk/online/story/0,3605,871013,00.html) [Accessed 16/01/03].

[87] Eaglesham, J. Blunkett backs down on state e-mail snooping. *FT.com*, 18/06/02. (URL: http://news.ft.com/home/uk/) [Accessed 16/01/03].

[88] Hargrave, S. There's a lot of it about. *The Guardian*, 07/10/02. (URL: http://media.guardian.co.uk/Print/0,3858,4516266,00.html) [Accessed 16/01/03].

[89] Lewis, P. Silent witness: the rise of CCTV and the fall of privacy. *Independent.co.uk*, 10/09/02. (URL: http://www.independent.co.uk/story.jsp?story=331928) [Accessed 16/01/03].

[90] Wolverton, T. Privacy groups target Amazon again. *News.com*, 08/10/02. (URL: http://news.com.com/2102-1017-961136.html) [Accessed 16/01/03].

[91] This Directive, approved in May 2002 by the European Parliament, replaces the EU Telecommunications Data Protection Directive 97/66/EC. Refer:

- European Communities. Commission. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*. Official Journal of the European Communities. No. L201/37. (31/07/02).

[92] Gardiner, J. Data traffic row intensifies. *Silicon.com*, 20/05/02. (URL: http://www.silicon.com/a53467) [Accessed 16/01/03].

[93] The Guardian. This morning UK law sees the biggest change in more than 300 years. *The Guardian*, 02/10/00, p.1.

[94] BBC News Online. Human rights in society. *BBC News Online*. URL: http://news.bbc.co.uk/hi/english/static/in_depth/uk/2000/human_rights/default.stm [Accessed 16/01/03].

[95] Davies, R. Human Rights Act boon for lawyers. *This Is London,* 02/10/2000. (URL: http://thisislondon.co.uk) [Accessed 16/01/03].

[96] The UK Data Protection Act 1998 was passed to implement the general Data Protection Directive 1995. In recitals 1 and 2, the Directive made explicit reference to the ECHR, including respect for the private domain. Thus the Data Protection Act 1998 has its roots firmly in the ECHR.

[97] Wadham, J. and H. Mountfield. *Human Rights Act 1998*, 1999.

[98] Michael, J. *Privacy and Human Rights: an international and comparative study with special reference to developments in information technology*, 1994.

[99] Arguably, this first generation of data protection legislation was initiated at the Nordic Conference - a meeting of legal authorities in Stockholm in 1967 which resulted in an influential, though not binding, declaration of the meaning of right to privacy. This is further discussed in Chapter 4.

[100] Michael, J., ref. 98, p. 133.

[101] Singh, R. Privacy and the media after the Human Rights Act. *European Human Rights Law Review*, 1998, 6, pp. 712-729.

[102] The case the author refers to relates to the privacy of mentally handicapped person who has been the victim of an offence: *X and Y v. The Netherlands,* Series A, No. 91 (1986) 8 EHRR 235, para.12. For an explanation of the referencing system regarding European Court of Human Rights cases, refer to Chapter 5, reference 7.

[103] For an alternative view, refer:

- Buxton, R. The Human Rights Act and private law. *The Law Quarterly Review*, 2000, 116, 48-65.

In the above article, Lord Justice Buxton argued that the HRA 1998 can only have effect in public law, and 'does nothing to create private law rights'. (p.65.)

[104] Elliot, M. Privacy, confidentiality and horizontality: the case of the celebrity wedding photographs. *The Cambridge Law Journal.* 2001, 60 (2), 231-3.

[105] This case concerned *Hello!* magazine's illicit photographs of Michael Douglas' and Catherine Zeta Jones' wedding. The couple had sold exclusive photographic rights to *OK!* for £1 million. The High Court had granted an interim injunction against Hello! publishing the photographs on 21 November 2000. This was lifted by the Court of Appeal on 23 November 2000.

[106] Jay, R. Data protection and human rights. *NADPO annual conference*, University of Warwick, 18-19 November 2002.

[107] Singh, R. and J. Strachan. The right to privacy in English law. *European Human Rights Law Review*, 2002 (2), pp. 129-161.

[108] For further details on *Campbell*, refer to ref. 28.

[109] Refer, for example:

- BBC News Online. 'Kiss and tell' footballer named. *BBC News Online*. 30/03/02. (URL: http://news.bbc.co.uk/1/hi/uk/1901566.stm) [Accessed 16/01/03].

[110] Refer to ref. 28 and Jay, ref. 106. Campbell will be appealing to the House of Lords.

[111] Great Britain. *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*. Statutory Instrument 2000 No. 2699, section 3. (URL: http://www.hmso.gov.uk/si/si2000/20002699.htm) [Accessed 16/01/03].

[112] *Draft Code of Practice: the use of personal data in employer/employee relationships*, ref. 36.

[113] Great Britain. *Anti-Terrorism, Crime and Security Act 2001*. London: TSO.

[114] Great Britain. Department of Trade and Industry. *Lawful Business Practice Regulations: summary of consultation responses*, October 2000. (URL: http://www.dti.gov.uk/cii/regulatory/telecomms/telecommsregulations/lawful_business_practice_summary.shtml) [Accessed 16/01/03].

[115] Great Britain. Cabinet Office. Performance and Innovation Unit. *Privacy and data-sharing: the way forward for public services*, 2002.

[116] Borley, J. Lord Chancellor's Department. Data-sharing to improve government. *NADPO annual conference*, University of Warwick. 18-19 November 2002.

[117] Clarke, R. Information technology and dataveillance. *Communications of the ACM.* 1988, 31 (5), 498-512.

[118] Cate, F.M. *Privacy in the information age*, 1997.

[119] Refer:

- Reidenberg, J.R. The globalisation of privacy solutions: the movement towards obligatory standards for fair information practices. *In*: C.J. Bennett and R. Grant (eds) *Visions of Privacy*, 1999, pp. 217-228;
- Reidenberg, J.R. Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review*, 2000, 52 (5), 1315-1371.

[120] Mohammed, E. An examination of surveillance technology and their implications for privacy and related issues - the philosophical legal perspective. *The Journal of Information, Law and Technology* [online], 1999 (2). (URL: http://elj.warwick.ac.uk/jilt/99-2/mohammed.html). [Accessed 16/01/03].

[121] Davies, S. New techniques and technologies of surveillance in the workplace, *Online Rights and Privacy at Work Conference* [online], London, 28/06/99. (URL: http://www.msf-itpa.org.uk/juneconf3.shtml). [Accessed 16/01/03].

[122] For full range of Baltimore 'content security products', refer: http://www.mimesweeper.com [Accessed 16/01/03].

[123] Malcolm, W. and D. Barker. Privacy and surveillance: trouble ahead for communications providers. *New Law Journal*, 2002 (7017), 80-2.

[124] *Anti-Terrorism, Crime and Security Act 2001*, ref., 113, section 102.

[125] *Ibid*, s.104.

[126] In the view of the OIC, retention of communication beyond that required for the communication provider's purpose (i.e. billing), is likely to be a breach of the DPA 1998.

[127] Roland Perry, director of public policy for the London internet Exchange (Linx), put the overall cost to ISPs and telephone companies at £40 million a year. Refer:

- Grossman, W. A new blow to our privacy. *The Guardian.* 06/06/02. (URL: http://www.guardian.co.uk/Print/0,3858,4427430,00.html) [Accessed 16/01/03].

[128] *Directive 2002/58/EC*, ref. 91.

[129] European Communities. Commission Press Room. *Data protection at work: Commission proposes new EU framework to European social partners*. Brussels, 31/10/02. (IP/02/1593).

[130] Simitis,S. Reconsidering the premise of labour law: prolegomena to an EU regulation on the protection of employees personal data. *European Law Journal*, 1999, 5 (1), 45-62. The author was a leading force behind Europe's first sub-national data protection law in Hesse, Germany.

[131] *Lawful Business Practice* Regulations, ref. 111, section 3.

[132] Smith, D. Assistant Information Commissioner. Data Protection: the Employment Practices Code. *NADPO annual conference*, University of Warwick. 18-19 November 2002.

The release of this Code has been repeatedly delayed owing to an extensive consultation and revision period lasting almost two years.

[133] See, for example:

- Inman, P. Email? You've got the elbow. Jobs and Money. *The Guardian*. 25/11/00, pp.2-3.
- Thompson, B. Every click you make. Online. *The Guardian*. 02/11/00, pp. 2-3.

# 4. Data Protection and the Law

## 4.1 Introduction

The development of data protection law within the UK, the EU and globally has been complex and varied. This Chapter focuses on the context and concepts of data protection legislation - in particular the processes leading up to the UK Data Protection Act 1998. It commences by defining the concept of data protection as a value distinct from the wider field of privacy. Section 4.2 charts the early development of data protection law internationally. This section commences with public concerns at the growth of large computer data banks with a capacity to store vast amounts of information concerning individuals, and concludes with nascent attempts to regulate this by large intergovernmental organisations such as the Council of Europe and the Organisation for Economic Cooperation and Development (OECD). These measures represented early attempts at international policy 'convergence', a theme first developed in Bennett's book *Regulating Privacy*[1].

International development of data protection law was strengthened from the early 1990's with the added input of the then European Economic Community (EEC). With divergent national approaches to data protection legislation threatening to distort the single market, and with increased data-sharing among member states following the Schengen Agreement, the EEC perceived a growing need to harmonise the disparate data protection legislation. Section 4.3 assesses the case for a general Directive and the structural reforms undertaken by the system of European governance at the time – transforming the EEC into the European Union (EU). This section concludes by outlining the provisions of the Data Protection Directive 95/46/EC, the Telecommunications Data Protection Directive 97/66/EC, and the latter's replacement – the Electronic Communications Directive 2002/58/EC, enacted in July 2002.

The remainder of this Chapter analyses various national attempts to legislate for information privacy. Section 4.4 assesses the early attempts made in Europe by the German Land (state) of Hesse (1970) and Sweden (1973) to legislate for information privacy. Additionally, German attempts to legislate at a Federal level, and the Netherlands' pioneering use of sectoral[2] codes of practice are considered. In all cases, analysis is comprehensive – charting a chronological course from the motivations to drafting the earliest laws to the need to update and reassess legislation in reaction to both national and international developments.

Section 4.5 assesses the UK experience in detail. Analysis commences with the first private members' bills on privacy drafted in the early 1960's, through detailed government papers and reports produced in the 1970's, concluding with the UK's first Data Protection Act, passed in 1984. Section 4.6 brings the UK experience up to date, charting attempts to implement an infrastructure for successful data protection, and gauging the privacy implications of the DPA 1998 – enacted to implement Directive 95/46/EC. Finally, organisational considerations are considered, with particular reference to the Employment Practices Code of Practice, currently being published in various sections by the OIC.

Section 4.7 considers the experience in North America. This is of vital importance for a number of reasons. Firstly, trading concerns, with the US being the UK's and EU's largest trading partner. Secondly, related to trade, employment considerations with a sizeable number of North American companies having subsidiaries based in the EU. Finally, in order for protection of personal information to be successful in the current globalised political and economic climate, the world's largest economy needs to be accommodated. The domestic experience of the US is considered, from judicial interpretations of the Constitution to the Privacy Act 1974 - drafted in response to domestic political scandal. Additionally, attempts to accommodate Directive 95/46/EU through a 'Safe Harbor' agreement - opposed by the current US administration – are analysed. The experience of Canada in this field serves as a contrast. Over a period of twenty years, Canada has steadily consolidated its data protection legislation, from patchwork state protection to a federalised structure under the

Personal Information Protection and Electronic Documents Act 2001 that has met with approval from the EU[3].

Finally, conclusions are offered – summarising the key findings from this Chapter.

### 4.1.1 Method

Desk research accounted for the bulk of the methodology in this chapter. Documents were analysed from organisations as diverse as the European Union (formerly Community), the UK government, the non-specialist press, consumer groups, and civil liberties organisations. However, use has been made of expert interviews – in particular those conducted with officials from the European and the UK government. The conclusions drawn will be tested during the fieldwork stage.

Most of the evidence analysed in this chapter was documentary – legislation, court cases, codes of practice, government consultation documents and European Union (EU) working papers.

### 4.1.2 Objectives

The objectives of this chapter are to:

- Set the Data Protection Act (DPA) 1998 in context with previous data protection and privacy legislation, both in the UK and abroad;
- Identify the main provisions of the DPA 1998 affecting individual data privacy, assessing whether the UK really does provide best practice in this area;
- Investigate the success of EU harmonisation, establishing whether (and how) the UK differs from other member states regarding data protection legislation;
- Analyse the relationship between the EU and the US, assessing the impact of the 'Safe Harbor' on the international transfer of personal data.

### 4.1.3 Definitions: 'privacy' and 'data protection'

The starting point for the debate about privacy and computers, when it commenced in the US and Europe in the 1960's, was the concept of 'privacy'. 'Privacy' has proved difficult to define, being more of a broad social value than a specific policy area, with different people having diverse notions of 'privacy'. However, many attempts have been made, from Judge Cooley's very wide 'right to be let alone' in 1888[4], to the International Commission of Jurists' Nordic Conference's catalogue of ten items in 1967[5]. In the UK, a concise working definition was posited by the Calcutt Committee on Privacy and Related Matters (1990)[6]:

> 'the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.'

This is close to the formulation in Article 8 of the European Convention of Human Rights (ECHR)[7], and extended beyond the protection of personal information. The definition of 'data protection', however, is more precise. According to Jay, it outlined:

> '(a) the standards to be applied when handling information about people, and;
> (b) the practices to be followed to achieve and maintain those standards.'[8]

This is the interpretation frequently encountered in organisational circles. It relates to the good practice policies of organisations in which protection is afforded through the prevention of hacking, unauthorised access, corruption of data, or other damage. 'Data protection' has been construed as data security and national data protection laws have frequently been merely a means of facilitating the use of personal data rather than protecting privacy. However, security is only one principle of 'data protection', and actually has less to do with the privacy interests of those whose data are held, and more with the organisation's functional

need to maintain confidentiality of information they hold against the risks of leaks or destruction[9]. 'Data protection' represents a reconciliation of values, especially between the claims of personal 'privacy' and the unimpeded flow of information between organisations within or between countries. Indeed, Raab[10] argued that 'data protection' can contribute to the achievement of non-privacy values such as public confidence in the police or other public organisations.

The overlap between the fields of 'privacy' and 'data protection' was identified by the Lindop Committee on Data Protection (1978) as 'data privacy' – 'the individual's claim to control the circulation of data about himself'[11]. This definition acknowledged the pioneering work of Westin and Miller, discussed in Chapter 3. It lends clarity to the concept, referred to in this thesis simply as 'data protection' in order to avoid any confusion.

## 4.2 The international scene: from guidance to legal enforcement 1967-1981

Much of present day interest in data protection stemmed from the growth of information technology and widespread concern over the potential for computers to intrude into the lives of individuals. During the 1960's and 1970's, a number of countries initiated studies on both personal data and individual privacy.

### 4.2.1 The Nordic Conference

In 1967, the Swedish section of the International Commission of Jurists (ICJ) hosted a conference on the issue in Stockholm[12]. An independent body of judges and lawyers[13], the ICJ lobbies for the promotion of human rights through research and by influencing policy-makers, particularly in intergovernmental organisations such as the United Nations and the Council of Europe. Their declaration concerning the meaning of the right to privacy listed ten specific rights. Some of the rights applied to data protection more closely than others. The last three rights referred to the need for the individual to be protected against:

(i) Interference with his correspondence;

(ii) Misuse of his private communications, written or oral;

(iii) Disclosure of information given or received by him in circumstances of professional confidence.

Although having no legal force, they were highly persuasive, being an important reference point in the national debates about the meaning of privacy and data protection that continued throughout the 1970's. In the UK, the rights were heavily drawn on in Brian Walden's Right to Privacy Bill 1969[14], the debate of which moved the government into commissioning the Younger Committee on Privacy in 1970.

Following on from the Nordic Conference 1967, there was a lot of activity in the international field concerning data protection. Discussions took place in the United Nations, the Council of Europe and the OECD. Some regulation of international data traffic was deemed necessary for two reasons:

(i) To avoid data users[15] evading a country's own data protection rules by processing abroad personal information about its own citizens;

(ii) To preserve the free flow of information against unilateral protectionist measures that may disrupt international trade.

It is the endeavours of intergovernmental bodies to provide regulation that will be analysed in the remainder of this section. During the period 1973-1981 two organisations were particularly active: the Council of Europe and the OECD.

### 4.2.2 The Council of Europe

The Council of Europe was formed in 1949 with the aim of bringing political cooperation for the advancement and protection of individual rights and freedoms throughout Europe. It was a pan European inter-governmental organisation – wholly distinct from the EEC, and in 1967 sent observers to the Nordic Conference. Its involvement was particularly significant, as the Council's

*Convention on Human Rights*[16] had been the one of the first European publications to make specific mention of the individual right to privacy. This was further developed, with the Council initiating a survey (1968-1970) on the legislation of its member states with regard to human rights and modern scientific and technological developments. The survey found that the existing law within member states did not provide sufficient protection for the citizen against intrusions on privacy by technical devices[17]. Legislation at the time touched on the protection of privacy from a limited point of view, such as secrecy of correspondence or the inviolability of the home.

Furthermore the Council found that the ramifications of the concept of privacy had never been established. It was 'doubtful whether the European Convention on Human Rights...offer[ed] satisfactory safeguards against technological intrusions into privacy'[18]. The survey noted, for example, that the Convention took into account only interferences with private life by public authorities, not by private parties. A particularly new threat to privacy came from the rapid growth and popularisation of computer technology. The ability of the computers to build up 'data banks'- collections or integrated networks of information capable of providing instantly, and over large distances, extensive data on individuals - was a major concern.

*Early Resolutions*

Following the survey, the Council set up a Committee on the Protection of Privacy vis-à-vis Electronic Data Banks. The Committee reviewed the situation in various member states, paying particular attention to the data protection laws in Hesse and Sweden. Following this, the Committee drafted Resolution (73) 22 - elaborating a set of principles concerning the protection of the privacy of personal information vis-à-vis electronic data banks in the private sector[19].

A year later, the Council of Europe produced Resolution (74) 29 on the protection of privacy of individuals vis-à-vis electronic data banks in the public sector[20]. This set out similar standards for processing in the public sector. The key difference between the Resolution (74) 29 and Resolution (73) 22 was that whilst

the latter did not include internal use of personal data (only the release of information to third parties), the public sector resolution found it difficult to distinguish between internal and external use. This was on the basis that in many member states all the branches of public administration were regarded as forming a whole, those different branches could not be considered 'third party' towards each other[21]. In both cases, the resolutions were drafted as recommendations to member states, taking into account both: 'the rapid development of computer technology and the urgency for European action before new divergences arise between the laws of the member states'[22]. It is significant that, at this early stage, harmonisation was seen as an issue. Indeed, Resolution (73) 22 mooted the possibility of a binding convention as a way of coping with the issue of transnational data banks[23]. At this stage, the two Resolutions in their own right influenced the drafting of data protection principles in various member countries, and resembled those contained in paragraph 34 of the 1975 UK White Paper *Computers and Privacy*[24].

*Convention 108*

In 1976, following on from the Resolutions on Electronic Data Banks, the Council of Europe established a Committee of Experts on Data Protection[25]. This body consisted of two experts from each member state, with the UK being represented by officials from the Home Office and the Central Computer Agency. Its terms of reference were defined in June 1977 and included a provision to:

> 'prepare a Convention on the protection of privacy in relation to data processing abroad and transfrontier data processing.'[26]

The work of this Committee was a natural continuation of the work carried out earlier by the Committee on the Protection of Privacy vis-à-vis Electronic Data Banks in order to both secure international solutions to an international problem, and to reinforce national legislation. The Committee of Experts had its first meeting in November 1976, with the OECD, EEC, Australia, the US and Canada among those enjoying observer status. Close liaison was maintained between the OECD both at the secretariat level and at the level of the Council of Europe's

Committee of Experts and its OECD counterpart - the Data Bank Panel, succeeded in 1978 by an expert group on transborder data barriers.

From November 1976 to May 1979, the Committee of Experts on Data Protection held four meetings, first under French chairmanship, then subsequently under that of the UK. The details were worked out by a working party of experts from ten member states, including the UK. The text was finalised in April 1980, and subsequently adopted by the Council of Europe. The Convention – number 108 – opened for signature on 28 January 1981. Since a wide geographical scope was considered essential in order for the Convention to be effective, Article 22 of the document fixed at five the number of ratifications by member states necessary for its entry into force. Therefore, as Table 1 below shows, the Convention did not enter into force until three months after ratification by Germany in June 1985. By 1990 – when the European Commission first drafted a general data protection directive - the number of ratifications had risen to 10. By mid-January 2003, this total had nearly trebled to 29.

| States | Date of signature | Date of ratification | Date of entry into force |
|---|---|---|---|
| Sweden | 28/01/81 | 29/09/82 | 01/10/85 |
| France | 28/01/81 | 24/03/83 | 01/10/85 |
| Spain | 28/01/82 | 31/01/84 | 01/10/85 |
| Norway | 13/03/81 | 20/02/84 | 01/10/85 |
| (West) Germany | 28/01/81 | 19/06/85 | 01/10/85 |
| United Kingdom | 14/05/81 | 26/08/87 | 01/12/87 |
| Luxembourg | 28/01/81 | 10/02/88 | 01/06/88 |
| Austria | 28/01/81 | 30/03/88 | 01/07/88 |
| Denmark | 28/01/81 | 23/10/89 | 01/02/90 |
| Ireland | 18/12/86 | 25/04/90 | 01/08/90 |

Table 3: Early ratification of Convention 108 by Council of Europe member states 1982-1990

Source: Treaty Office, Council of Europe at http://conventions.coe.int

The Convention was significant as it represented the first attempt at European-wide data protection legislation. The preamble clearly stated that its aim was to reconcile the need for privacy embodied in the ECHR Article 8 with free trade. Furthermore, like the ECHR, this measure was binding on contracting states. However, unlike the ECHR, Article 23 of Convention 108 was drafted with a view to allowing the accession of non-member states to the instrument[27]. Indeed, the explanatory report to the Convention stated that in this respect it was not advisable to rely solely on the ECHR for data protection, as it is a 'closed instrument' – not permitting the participation of non-European and non-member states[28].

The Convention had three main purposes:

(i) To establish minimum standards of data protection which contracting states would undertake to enforce internally;
(ii) To define special rules on transborder data flows;
(iii) To facilitate mutual assistance and cooperation between national data protection authorities.

The principles, found in Chapter II of the Convention, owed much to the principles laid down in the earlier Council of Europe Resolutions on data banks – (73) 22 and (74) 29, and, to legislative developments in member states[29]. They were to form the common core in the domestic legislation of contracting states, and were as follows:

(i) Fair and lawful obtaining and processing of personal data;
(ii) Storage of data only for specified purposes;
(iii) Personal data should not be used in ways incompatible with those purposes;
(iv) Personal data should be adequate, relevant and not excessive in relation to the purposes to which the data are stored;
(v) Personal data should be accurate and where necessary kept up to date;
(vi) Personal data should be preserved in identifiable form for no longer than is necessary;
(vii) There should be adequate security for personal data;

(viii) Personal data should be available to be accessed by individuals who have rights of rectification and erasure.

Whilst the Convention gave clear and precise instructions as to the purpose to be achieved by each principle, the manner of implementation in domestic law was left to each member state. Chapter III – concerning transborder data flows – aimed to reconcile the simultaneous and often competing requirements of free flow of information and data protection. The main rule was that transborder data flows between contracting states were not to be the subject of any special controls[30]. Thus, this avoided the principle of free flow of information being jeopardised by any form of protectionism.

Finally, Chapters IV and V provided the mechanisms for cooperation between contracting states. The former concerned individual cases, for example mutual cooperation between authorities and assistance to data subjects abroad. Chapter V concerned cooperation with regard to the Convention as a whole. A Consultative Committee was set up on enactment of the Convention, consisting of two representatives from each contracting state. Their role was purely advisory, putting forward opinions and proposals concerning the application of - and amendments to - the Convention.

States were not to ratify the instrument until they had national law in place guaranteeing compliance with standards set out in the Convention[31]. In effect, until states could give such guarantees, they ran the risk of having trade barriers erected against them or alternatively becoming 'data havens' for those wishing to avoid the data processing regulations. It was this threat of trade barriers, more than any regard for individual privacy, that was to galvanise the UK government into action[32]. In 1984, the UK passed the Data Protection Act, finally ratifying the Convention in August 1987.

### 4.2.3 The Organisation for Economic Cooperation and Development (OECD)

The Organisation for Economic Cooperation and Development (OECD) is an international organisation whose primary aims are to foster economic stability and encourage trade. It was initially founded as the Organisation for European Economic Cooperation in 1948 with the aim of coordinating national economic policies in post-war Europe. In 1960, as other European institutions took responsibility for economic cooperation, it transformed into an international trading body with the accession of Canada and the US. In 1964, Japan became a member with Australia and New Zealand subsequently gaining membership.

*The OECD guidelines*

Until 1978, OECD work in the field of data protection was conducted by the Data Bank Panel, which considered data protection among other issues. However, the implications of the proposed Council of Europe Convention forced the OECD to reconsider its priorities in this field. During a seminar on Transborder Data Flows and the Protection of Privacy in September 1977, the non-European participants expressed concern that the Convention would lead to restrictions being placed on the export of personal data to non-contracting states[33]. Such discrimination had already occurred as a result of national legislation. The Swedish Data Inspection Board, for example, had been particularly strict in controlling the export of personal data to countries without similar data protection laws. Swedish organisations had sometimes been refused permission to export data to processing by UK service companies[34], and in 1995 American Airlines was prevented from transferring passenger meal preference data that could reveal religious convictions (for example, kosher food) to the US for processing[35].

Therefore, to protect the requirements of its wider membership, the OECD embarked on a separate drafting exercise of its own. The Data Bank Panel was replaced with an Expert Group on Transborder Data Barriers and Privacy Protection, which first met in April 1978. Its terms of reference included:

> 'develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonisation of national legislation, without this precluding at a later date the establishment of an international convention.'[36]

The latter part of the statement was significant, with the option of a joint Convention a further indication of the close cooperation and consultation at an international level with the Council of Europe and the EEC.

In 1980, the OECD adopted recommendations in relation to data protection[37]. Perhaps the weakest of data protection instruments issued at this time, the OECD Guidelines focused on eight general principles, based broadly on those set out by the UK Younger Report (refer to section 4.5.1 of this Chapter). The principles dealt with matters such as: limiting the amount of information collected; ensuring its accuracy and quality; ensuring the restriction of its use to the purpose specified; provision of adequate safeguards for the secure storage of personal data; permitting individuals to check access to the validity of personal data; and requiring the accountability of the operators of data banks for those stores of personal information. The preamble emphasised the concern that national moves to protect privacy might create unjustified barriers to trade, and recommended that member states take account of the guidelines in their domestic legislation in order to overcome the possibility of trade barriers. This point is vague in its requirements, supporting both legislation and self-regulation. Nevertheless, it does require both `reasonable means for individuals to exercise their rights' and 'adequate sanctions and remedies in case of failures to comply'[38].

Applicable to both public and private sectors, the Guidelines recommended that transborder data flows should not be restricted to other member states. An annual review of national progress was also instrumented. Yet, there was no formal process to ratify or adopt the OECD Guidelines. As such the Guidelines had little influence within Europe, with EEC states, as shown in Table 2, implementing Convention 108. However, the Guidelines have proved popular as a forum for the discussion of data protection issues among the wider international community. They were accepted immediately by the US and have been widely referred to in

Canada as a basis for its self-regulatory instruments, culminating in the Canadian Standards Association's 1996 Model Code for the Protection of Personal Information[39]. Moreover, they have stood the test of time, and have since been under active development by the OECD's Group of Experts on Security and Privacy, particularly in relation to international networks[40].

## 4.3 'Top down': the role of the European Commission 1985-2003

### 4.3.1 Context: The European Economic Community (EEC)

The European Economic Community (EEC) was formed in 1957 – developing out of the European Coal and Steel Community which had been founded six years earlier. The EEC comprised six founding states – France, Germany, Italy, Belgium, the Netherlands and Luxembourg. On 1 January 1973, the UK, Denmark and Ireland acceded, increasing membership to nine.

| **Date** | **Country** |
|---|---|
| 25 March 1957 | Belgium |
| | France |
| | Germany |
| | Italy |
| | Luxembourg |
| | Netherlands |
| 1 January 1973 | Denmark |
| | Ireland |
| | United Kingdom |
| 1 January 1981 | Greece |
| 1 January 1986 | Portugal |
| | Spain |
| 1 January 1995 | Austria |

| | |
|---|---|
| | Finland |
| | Sweden |

Table 4: Accession of member states to the European Community

Source: Weidenfeld, W. and W. Wessels. *Europe from A to Z – guide to European integration.* Luxembourg: Office for Official Publications of the European Communities, 1997.

The debate on data protection in the EEC during the period 1973-1981 turned on the relationship between the Commission of the European Communities (hereafter the European Commission) – the institution that proposes, and then enforces EEC legislation – and the European Parliament, which during this period had a largely advisory role[41]. The Commission first expressed an interest in data protection in 1973, arguing that it would be better to establish common ground rules at an early stage than have subsequently to harmonise conflicting national legislation[42]. In 1974 it sought the views of the European Parliament on the matter. According to Mellors and Pollitt, it was 'the first time that it had asked for guidance from the Parliament before drafting a directive'[43]. The Parliament responded by passing resolutions in 1975 and 1977 calling on the Commission to prepare a directive on safeguards for privacy. By 1976, the Commission had set up its own Group of Experts on Data Processing and the Protection of Privacy, a body on which the UK was represented by Home Office officials. This group commissioned a study into transborder data flows, the possible distortion of competition, and data security. However, in 1980, the European Commission chose to merely address a Recommendation to Member States[44] that they should ratify the Council of Europe's Convention 108 before the end of 1982.

The European Community was thus a latecomer regarding data protection measures. In fact, it was factors from outside – particularly trade - that prompted the Commission to submit its first proposal for a Directive in 1990. The issues surrounding the move towards a Directive will be analysed in this section, along with the key provisions of the Data Protection Directive 95/46/EC[45], finalised in 1995. A sister Directive, concerning data protection in public telecommunications[46], was enacted in 1997, and revised in 2002. Both Directives had, and still have, wide-ranging implications for the member states.

### 4.3.2 The case for a general Directive

*Different national approaches*

The implementation of Convention 108 had been hampered by the lack of compulsion. Compliance was very slow with only seven EC countries ratifying the instrument up to 1990[47]. Moreover, those that did - by introducing appropriate national laws - had such a diversity of approaches that there was a complete lack of consistency in the legislative framework within the Community. Differences in legislation were manifold: the UK, Irish and Swedish laws did not include manual records, whilst those of Germany and France did. Some laws – for example in France - prohibited the collection and storing of certain types of sensitive personal data, whilst UK law merely permitted additional protection for sensitive data at the discretion of the Secretary of State. German law did not recognise sensitive data at all. Finally, subject rights varied. All laws required the data user to pass a copy of data to a data subject should he request it. However, Germany, the Netherlands, and France, for example, required that the data user informed the data subject that data about him was being held, whilst no such obligation existed in the UK and Ireland.

Additionally, interesting differences occurred on the question of exemptions from the statutes. German law specifically exempted personal data processed for journalistic purposes; French law specifically exempted personal data in the public domain; whilst most laws exempted data collected for personal or domestic use from requirements under their legislation. Bennett (1992) sought to find explanations for such policy 'divergence' by analysing domestic characteristics of the countries he studied[48]. These explanations were: the repertoire of policy instruments within the state; the preferences of dominant social groups; the role of the political parties in electoral competition; the position and power of bureaucracy; and economic constraints. A mixture of these influences can be seen in each of the states analysed later in this Chapter.

By 1992, all European Community members states bar Italy and Greece had enacted data protection legislation. Yet, the significantly different approaches taken by these states magnified the need for harmonising legislation from the 'top down'.

*The European single market*

Moreover, the situation distorted the Commission's aim of achieving a single market. As the 1980's progressed, concerns about free trade increased in prominence. The uneven laws created potential obstacles to the free flow of information and additional burdens for 'economic operators and citizens'[49]. By the early 1990's, companies were required to register or be authorised to process data by supervisory authorities in several member states, to comply with different standards, and were restricted from transferring data to other EU member states. The fears of a decade earlier that trade barriers would be erected based on differential privacy protection in member states were being realised.

The concerns of business were crystallised by the *Fiat* case in 1988, which according to Burkert[50], prompted the European Commission to begin serious work on a data protection instrument. The *Fiat* incident was sparked by the refusal of the French Data Inspection Commission to allow the transfer of personal data about *Fiat* managers from their subsidiary in France to the parent company in Torino, Italy. France had a data protection law at that time; Italy did not, nor had adopted Convention 108. Consequently, the French Commission insisted that *Fiat* Italy made a written representation that the French Data Protection Act and Convention 108 governed the data transfer. This case clearly highlighted the potential for disruption to the operation of the internal market.

Additionally, there were increased public concerns at the accumulation of personal data beyond national boundaries, with information concerning the citizens of one member state increasingly being processed in other member states of the EU. Spurred on by the above factors, work on a data protection directive began in earnest in 1990 - two years prior to the enactment of the European single market.

The aim was to enact legislation that removed obstacles to the free movement of personal data whilst still guaranteeing the protection of individual privacy.

*The Schengen Agreement*

A further stimulus towards a general data protection directive was provided by the Schengen Agreement, regarding the abolition of internal borders between certain European Community member states and cooperation in policing. The orginal Agreement was signed between France, Germany, Belgium, Luxembourg and the Netherlands in 1985. Although an instrument outside Community law, it was politically associated within the Community, and demanded data protection considerations. Raab and Bennett viewed the 1990 Schengen Convention, which built on the Agreement, as key in driving overall integration of the European Community[51]. This focused on issues of law and order, law enforcement and national security including terrorism, drug trafficking, asylum seeking, visas and extradition. At the heart of the Schengen mechanism was the Schengen Information System (SIS) – a universal computerised investigation and information system to aid the fight against cross-border crime. The SIS allowed all police stations and consular agents from the Schengen group to access data on specific individuals, or vehicles and objects that had been lost or stolen. Although not involving all members states of the European Community[52], it nevertheless posed acute issues of privacy protection across national borders. Anxiety about the exchange of sensitive criminal information meant that each Schengen country had to enact legislation at least equal to that level in Convention 108 and the Council of Europe's 1987 Recommendation on police data[53].

Yet, there was an absence of a central supervisory authority - leaving important controlling, verifying and troubleshooting functions unperformed. In 1991, data protection commissioners from eight European Community states[54] declared Schengen's provisions 'coherent', but reaffirmed absolute necessity of national enforcement arrangements before Schengen entered into force[55]. This added to the climate at a time when the European Commission was drafting a directive on data protection.

*From Community to Union: structural reforms*

In 1990, the Commission published its first proposal for a directive[56], which took another five years to be finalised. During that period, the focus shifted from a text designed primarily to protect individual rights, whilst preventing barriers to the free flow of personal data, to more balanced approach. This move can be seen in the change in titles of the proposed Directive. The first draft related to:

> Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data.

However, following amendments tabled by the European Parliament and complaints that the original draft was over-reliant on German data protection law[57], a second proposal (which became the actual Directive) was published in 1992. Its title reflected the move towards a harmonising text:

> Amended proposal for a Council directive on the protection of individuals with regard to the processing of personal data *and on the free movement of such data*[58]. [Author's italics].

The debate surrounding the Directive took place during a period of rapid reform within the European Community. The European Treaty had been revised at Maastricht[59] in February 1992, and came into force in November 1993. Under this treaty, the European Union (EU) was founded as an overarching legal structure – comprised of three pillars: the European Communities[60]; common foreign and security policy; and justice and home affairs. Among the amendments, the treaty wrote new principles of citizenship and subsidiarity, and established new decision-making procedures. Following Maastricht, the European Parliament was able to play a more significant role. Parliament obtained the right to approve the appointment of each new European Commission, and to become more involved in the legislative process due to the introduction of a complex new co-decision procedure by Article 189b. Legislation introduced through this procedure needed approval of Parliament to be adopted.

The process is ongoing. Further amendments were made with the Treaties of Amsterdam (1997) and Nice (signed February 2001)[61]. Amsterdam was significant for several reasons. Firstly, it extended co-decision procedure to all areas of decision-making except economic and monetary union[62]. Secondly, a new stress on human rights and democracy was encouraged. Thirdly, Amsterdam integrated the Schengen Agreement. Moreover, Amsterdam inserted a new Article into the original European Community Treaty of 1957, making the rules on protection of individuals applicable to the Community institutions themselves[63]. The new Article 286 provided that from 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data applied to the Community institutions and bodies. Additionally, it provided for the establishment of an independent supervisory body responsible for monitoring the application of those Community acts to Community institutions and bodies. Measures harmonising data protection laws had reached the heart of the European Community.

### 4.3.3 Data Protection Directive 95/46/EC: key provisions

The Directive was finally adopted in October 1995, with member states required to implement the measure into their national laws by 24 October 1998. The UK complied with its obligations by passing the Data Protection Act 1998, which entered into force on 1 March 2000. The Directive can be seen as a general framework legislative provision which has two aims:

(a) protection of an individual's privacy in relation to the processing of personal data;

(b) harmonisation of data protection laws of the EU member states[64].

Member states could not, therefore, restrict or prohibit free flow of personal data to other members states on grounds of unequal protection[65]. This would avoid a repeat of the 1988 *Fiat* dispute between France and Italy. Some of the terminology changed, too, with those processing, holding and using the data - known in the UK DPA 1984 as 'data users' – being called 'data controllers'. The

terms of the Directive were more precise, and applied to both the public and private sectors. The legislation introduced features from national data protection laws, for example, codes of conduct from the Netherlands and the concept of an internal (company) data protection officer from Germany. Jay[66] identified seven significant features that separated the Directive from earlier data protection instruments:

(i) It applied to some manual files;
(ii) It set out requirements for the legitimate processing as threshold requirements;
(iii) It required specific controls for processing of sensitive data;
(iv) It provided for extensive individual rights, beyond those of access and rectification;
(v) It restricted transborder data flows outside the Community to those states without adequate protection;
(vi) It provided exemptions for journalistic, literary and artistic purposes;
(vii) It significantly strengthened the security requirements for processing.

One of the main features of Directive 95/46/EC was the extension of data protected to cover manual records. The first reference to manual data appears in Article 2(b), describing processing of personal data as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means'. The use of the word 'any' clearly emphasised every conceivable operation on personal data is 'processing' (e.g. from collection, use, and disclosure, to storage and destruction). This had wide-ranging implications. Article 3 of the Directive restricted the definition of manual processing to data intended to be part of a 'filing system' (i.e. organised, or intended to be organised in a structured manual file).

The criterion concerning legitimacy was also a significant addition, recognising that every form of processing of personal data is to be regarded as an intrusion upon the fundamental freedoms and right to privacy of a person – therefore requiring legitimacy. This could come from the unambiguous consent of a data subject, from a legal provision, from the necessity of a performance of a contract,

or a task in the public interest, or in order to protect the vital interests of the data subject[67]. An example of vital interests would be if the data subject's life was in danger, and it was impossible to gain his consent to access his medical records.

Sensitive personal data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life were especially heavily protected[68]. A key element of protection of personal privacy, under this provision such data could now only be processed under specific conditions, including with the 'explicit consent' of the data subject. It is not clear where the distinction lies between the data subject's 'unambiguous' consent for legitimate processing of data (Article 7(a)) and 'explicit' consent for more sensitive material. However, sensitive data can be accessed by third parties if required by national employment law, or if 'manifestly made public by the data subject'[69]. An example of the latter would be if a person revealed their political loyalties in a letter to a newspaper.

The data subject had extended rights set out in Articles 10-12, and 14. In addition to rights of access and rectification, these included rights:

- To information about the processor, the recipients and purposes of the processing operation;
- To have incomplete data erased or blocked;
- To object to data being processed for the purposes of direct marketing;
- Not to be subject to a decision that has legal effects and which is based solely on automated processing of data;
- To stop data controllers processing data which would cause distress or damage to the data subject;
- To compensation if distress or damage has been caused due to contravention of requirements of Directive.

The Directive also set out the conditions under which personal data may be transferred to countries outside the European Union. In general, a transfer may only take place if a third country ensured an adequate level of protection for the rights and freedoms of the data subjects. The impact of this on global transfer of

data are discussed in section 4.7 of this Chapter, with particular reference to the 'Safe Harbor' principles agreed between the EU and the US. Finally, Article 29 of the Directive established a Working Party on the protection of individuals with regard to the processing of personal data. This was to give the Commission an opinion on the level of protection in third countries and examine any questions covering the application of national measures adopted in the Directive in order to contribute to the uniform application of such measures[70]. Parallel to this, Article 31 established 'The Committee', comprising representatives of member states. If there is a data protection problem, the Commission representative submits draft measures to be adopted; the Committee then deliberates and delivers its opinion. In this way, initiatives or opinions arising from Working Party concerns can be reported to the Commission, considered by the Committee, and adopted if agreed. Once adopted, the measures 'shall apply immediately'[71].

Nevertheless, some transitional exemptions were specified in Articles 32 and 33. Following on from the deadline for implementation of 24th October 1998, a delay of up to three years was permitted with respect to manual personal data the processing of which was 'under way' at that time. Yet, no lag has been permitted in regard to processing beginning after that time - even if processed in a manual system. Moreover, there was a nine-year delay (until October 2007) to the application of three Articles with respect to personal data already held in manual filing systems. The Articles in question are: Article 6 - the data protection principles; Article 7 - regarding lawfulness of processing; and Article 8 - sensitive personal data. Such postponements could, argued Carlin[72], encourage the creation of data havens that the Directive sought to eliminate. If the UK allowed exemptions for existing files to run for the full twelve years, some controllers may be tempted to centralise their manual files within the UK. However, in creating the Data Protection Working Party, Commission sought to minimise the potential for such divergences in national legislation.

Yet, in spite of the more precise regulations, common problems still existed with the general Directive. When considering the criteria for legitimising data processing (Article 7), it was difficult to identify a general principle behind the term 'consent'. As Blume[73] has stated, such a term presupposes that the citizen is

both informed and able to freely decide whether he wants to give his consent. If not, the notion of consent could be an illusion, making privacy dependent on other conditions. Essentially, formal data protection law was not the final word in the fight for privacy of personal data, just the starting point. As studies by Rule[74], Raab and Bennett[75], and Raab *et al*[76], among other academics, have demonstrated information privacy can only be guaranteed by implementation of a full data protection infrastructure. Opinions differ on the exact criteria required to ensure compliance. However, factors may include: a strong proactive supervisory authority; an educated and interested citizenry; and detailed rigorous application of data protection principles by the organisations that process individuals' personal data. It is the final factor that will be assessed in some detailed in the case study analysis of this thesis (Chapter 7).

Finally, concern was expressed at a possible reduction of the level of protection in states such as Germany and Sweden. This appeared foreclosed by Recital 10 in the Directive: 'the approximation of those [national] laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community'[77]. Yet there are still inconsistencies. In many states, the press and media exemptions have to be reassessed, with Germany, for example, against general privilege for the media.

The success or otherwise of harmonisation of data protection laws is currently being assessed by the European Commission[78]. The initial implementation of the Directive was slow. Of the 15 member states, only Sweden and Greece had data protection legislation fully in force by the 24 October 1998 deadline. By January 2003, over four years after the deadline for implementation, two EU states – France and Ireland - had still to put the Directive fully into operation[79]. Nevertheless, with 13 member states having implemented Directive 95/46/EC, it appears that in terms of implementing the relevant legislation harmonisation is being achieved. Issues surrounding implementation of the Directive's provisions at ground level in a sample of member states, including the UK, are considered in sections 4.4 and 4.6 of this Chapter.

### 4.3.4 Telecommunications Data Protection Directive 97/66/EC

The Telecommunications Data Protection Directive 97/66/EC was applicable to processing of personal data in public telecommunications, in particular, in the integrated services digital networks (ISDN) and public digital mobile networks. These communication systems facilitated the wide ranging storage of data concerning, for example, identity of callers, duration of calls, identification of phone numbers, identification of incoming and outgoing calls and the profiling of teleshopping details. Under Directive 97/66/EC, data subjects had the right to prevent processing of the above data for marketing purposes, but had to accept the storage of data for connection and accounting purposes. Finally, the Directive prescribed obligations for the member states to take care of liability rules and sanctions and extended the protection of data to legal persons (companies). The Data Protection Working Party's terms of reference were extended to clarify questions arising from the application of Directive 97/66/EC.

#### *Electronic Communications (E-Communications) Directive 2002/58/EC*

In July 2002, the European Commission approved a successor E-Communications Directive[80], replacing Directive 97/66/EC. Member states have until 31st October 2003 to bring the new Directive into effect. The aim of Directive 2002/58/EC is to provide technology neutral legislation in the telecommunications sector. It has been drafted so that it is applicable to all types of electronic communications, and it includes the following key provisions:

- *Unsolicited communications*: a harmonised opt-in consent to unsolicited commercial email and SMS messages to mobile telephones[81];
- *Cookies*[82]: users should be provided with clear and comprehensive information on their purposes and have the right to refuse them;
- *Directories*: subscribers must be given the choice as to whether their details appear in a publicly available printed or electronic directory, plus rights to verify, correct or withdraw their data;
- *Location data*: information concerning the geographical location of a user of or subscriber to a mobile telephone must not be processed without the

consent of the relevant person. Even where consent has been given, users and subscribers must be given the opportunity to both permanently withdraw such consent at any time and to temporarily switch off the telephone or network's ability to track the location of the mobile telephone.

Controversially, member states may legislate for a 'limited period' to restrict the scope of protections offered under the Electronic Communications Directive to safeguard national or public security, defence, and to prevent, detect and prosecute crime when 'necessary, appropriate and proportionate' within a democratic society. These measures must be in accordance with the ECHR and the rulings of the European Court of Human Rights. Nevertheless, this aspect has proved controversial with civil liberties groups as it overturns part of the Directive 97/66/EC permitting data retention only for business purposes, for example billing[83]. Additionally, concerns have been expressed about the extra cost of data retention for businesses[84].

Directive 2002/58/EC will provide greater harmonisation within Europe in the context of electronic communications. The opt-in provision for email and SMS marketing will have a dramatic effect on e-commerce businesses, as these organisations will have to alter their websites to take opt-in consent – as opposed to the commonly existing opt-out consent - from users. This has been widely welcomed by consumer groups, but not by the Union of Industrial and Employers' Confederations of Europe (UNICE) which stated that the provision does not achieve the goal of curbing spam as 'most spam originates from outside the EU and opt-in thus only puts legitimate European business at a competitive disadvantage'[85].

## 4.4 Europe: divergence to convergence

During the period 1967 to 1978, there was considerable activity within European Community states on the area of data protection. The German Land of Hesse initiated the world's first data protection law in 1970. In 1973, Sweden became the first country to enact a national data protection law. In the following five

years, five more European countries were to follow suit. By 1978, the data protection laws of Hesse and Sweden were being amended. However, two decades would pass before data protection was harmonised at a European Community level. In the interim, a multitude of national data protection laws (see Table 3 below) resulted in a diverse regulatory environment within the European Community.

| Year of enactment | Country | Legislation |
|---|---|---|
| 1973 | Sweden | Personal Data Act |
| 1977 | (West) Germany | Federal Data Protection Act |
| 1978 | France | Act on Data Processing, Data Files and Individual Liberties |
| 1978 | Denmark | Private Registers Act<br>Public Authorities' Registers (Consolidation) Act |
| 1978 | Norway | Act relating to Personal Data Registers |
| 1978 | Austria | Data Protection Act |
| 1979 | Luxembourg | Act concerning the Use of Nominal Data in Computer Processing |
| 1984 | United Kingdom | Data Protection Act |
| 1988 | Ireland | Data Protection Act |
| 1988 | Netherlands | Data Protection Act |
| 1992 | Belgium | Law on Privacy Protection |

Table 5: European national data protection legislation prior to EU Data Protection Directive 1995

Source: Data Protection, Directorate General Legal Affairs, Council of Europe[86].

This section analyses data protection laws of Hesse, Sweden, Germany and the Netherlands. These statutes were selected for a couple of reasons. Firstly, Hesse, Sweden and Germany were among the states and countries to draft the first generation of data protection statues. They were laws drafted in response to various national pressures, largely free from influence by international bodies such as the Council of Europe, the OECD and the European Commission. Secondly, those laws, together with the Netherlands' Data Protection Act (not passed until 1988) exemplified different national approaches to the problem of regulating data

users. Such disparities resulted in the diverse regulatory environment that was to compel the European Community to act to harmonise data protection from the beginning of the 1990's. It is useful to gain detailed context to this process. However, this discussion has not been limited to four countries. The UK DPA 1984, an example of a registration approach, is assessed in section 4.5. Finally, the North American response to data protection concerns is considered in section 4.7.

Bennett argued in 1988 that these differences in national approach stemmed from domestic constraints – based on administrative, historical and cultural factors - filtering out unacceptable options[87]. This section will study these domestic constraints. Three main considerations underlie the analysis of national data protection legislation in this section. Firstly, how such diverse approaches to data protection legislation emerged from the public concerns about privacy of personal information in the 1960's and 1970's. Secondly, the way the laws influenced the drafting of Directive 95/46/EC. Thirdly, the process of convergence, as national laws were modified, and harmonised, after 1995 to accommodate the provisions of the Directive.

### 4.4.1 Hesse: the first data protection law

In Hesse, the Data Protection Act (DPA) served two main interests. Firstly, it aimed to prevent the violation of individual privacy arising from the introduction of a new public computing systems. Indeed, the DPA had been introduced to mitigate the provisions of another Act authorising a state and local data processing network[88]. Effectively, a measure to extend public sector processing had been accompanied by a piece of legislation safeguarding privacy. Secondly, the DPA 1970 addressed the possible shift in the constitutional balance of powers due to the 'information advantage' enjoyed by the executive over the parliamentary organs. Local communities feared what they saw as the inherent centralising power of the executive machine would shift their traditional power and influence to the Land[89]. This fear was allayed by section 6 of the Act which allowed the Land parliament and local representative bodies the right to information that did not contain

personal data. For the parliament, this was reinforced by the provision in section 5 (3) stating:

> 'As a rule public interest shall not stand in the way of the Land parliament's right to information.'[90]

The original Act was therefore wide in scope – extending beyond personal data to combine the function of a data protection law with those of a limited freedom of information law.

The Hesse Data Protection Act 1970 therefore dealt with computerised data held by local and public bodies within the Land's jurisdiction. The Act laid down penalties for the examination, alteration, extraction and destruction of data by unauthorised persons. The data subject had a right of access, a right of correction of inaccurate data and the possibility of obtaining an injunction and remedies in the case of unlawful processing. Moreover, a Data Protection Commissioner was appointed to oversee the handling of information provided by individuals and to consider complaints. However, the Commissioner had no decision-making power. As the Data Protection Commission regulated the public sector, it was crucial for it to be seen to be independent of the government. To this end, the Data Protection Acts of Hesse declared its data protection authority not to be subject to direction from the Land government in the exercise of its duties. Furthermore, it was answerable to the legislature rather than the executive. Thus, the Commissioner was appointed by, and reported to, the Hesse parliament and acted at its behest to investigate a refusal by the executive to release information. In the successor Act of 1978 (section 30), this independence was strengthened further by manning the Commissioner's office from the Parliamentary staff rather than, as previously, from the Prime Minister's office. However, the absence of a specific registration requirement hampered the Commissioner's work to such an extent that this requirement too was added to the 1978 Act[91].

Although the initial 1970 Act was limited in terms of subject rights, it did establish some of the basic elements for future legislation. Firstly, it influenced German and later European terminology – with its usage of terms such as 'data protection'

for the protection of the rights of persons who data was being handled, and the term 'commissioner' for the ombudsman who oversaw the application of the law. In Simitis, Hesse had a long-standing Commissioner who, during his sixteen years in office (1975-1991), saw his job as being highly political – emphasising the need for cooperation with the media, the public and the legislature[92]. Without support of these partners, crucial for the policy process, effective data protection would become virtually impossible.

Secondly, the Hesse Act set out some basic themes for the forthcoming legislation in Europe. Burkert[93] identified four:

(i) *The negative default rule* – that the processing of personal data was seen as interference per se that needed legitimisation;

(ii) *The rights of the data subject.* For the first time, data subjects had a right of access to information relating to them without the need to show any reason as to why they wanted access;

(iii) *The omnibus approach.* Although, due to reasons of legislative competence, the Hesse Act could not cover the private sector, it set out to regulate all of the state public sector (within its jurisdiction);

(iv) The establishment of a *supervisory authority.*

Essentially, the Act expressed what Burkert called the 'regulative philosophy'. Regulations established to influence behaviour were backed up by institutions to take care of the individual's interests, even if the authority was closely linked to the infrastructure of the state that was being supervised[94].

### 4.4.2 Sweden: the first national data protection law

In Europe, Sweden pioneered the use of computers in public administration. In 1963, the Swedish Agency for Administrative Development was charged with overall coordination of computer policy. By 1969, plans for a computerised population register were announced amidst significant public unease. The

development of the central population register was suspended by parliament in April 1972, pending the report of the Royal Committee on Publicity and Secrecy. The recommendations of this Committee were incorporated into the 1973 Data Act, the first national legislation of its kind. In this Act, privacy protection was balanced with the public right to know. Sweden had a long tradition of freedom of information extending back to the Freedom of Press Act 1766[95]. The right of the individual to have access to government files about himself was reinforced and extended to computerised records kept by the private sector. At the same time privacy was to be protected by controlling access to such records by third parties.

As in Hesse, the Swedish statute extended only to automated records. However, the Swedish system was regulated by the powerful Data Inspection Board (DIB) – which granted extensive licensing powers and was able to draw up detailed rules for particular users and classes of user. Sections 5, 6, and 10 of the Data Act[96] set out the basic data protection rules (for example, right of legal access by data subjects). Yet, most of the rules – what data may be processed, how it may be used, to whom it may be disclosed – were determined by the Board, with organisations requiring DIB's permission to process personal data. The need for a licence also meant that the essential characteristics of record systems were rendered transparent, thus enabling oversight of the automatic processing of personal data from the earliest collection stages, to its organisational uses and its disclosure elsewhere. In this way, the Swedish approach was anticipatory – with the legislation based on the assumption that the computer would raise further problems requiring additional regulation. A similar system of licensing was later established in France with the enactment of its Act on Data Processing, Data Files and Individual Liberties (refer to Table 3 on page 99).

The Swedish Data Act 1973 was unique in making no distinction at all between the public and private sectors. The only sector singled out in the statute was the class of data bank which had been legally established. Following approval in 1976 for a computerised central population register, the Swedish parliament in 1977 introduced a new section to the Data Act limiting the number of privately owned population files. Data banks were exempted from the usual requirement to obtain authorisation from DIB, although any further legislation resulting in a new

databank had to be submitted to DIB for an opinion[97]. Overall, DIB proved very successful at keeping costs down, but its staff doubled in the first five years from fifteen to thirty, and the revised Act of 1978 simplified the procedure for licensing routine applications.

The high profile of DIB during the late 1970s and early 1980s was in no small part due the role of its flamboyant Director General, Freese. Indeed, Flaherty described Freese as 'the most important single influence on the development and implementation of data protection'[98]. That may be an overstatement, given that the Swedish Data Acts enabled the Director General to wield a large stick. Yet, from his appointment in 1977 to his departure in 1986, there is no doubt that Freese proved willing to take a robust public position on matters affecting data protection. In particular, he was strongly opposed to record linkages (or data matching) involving Sweden's numerous automated public and private sector data banks. In this respect, his main concern was with the quality of the data used and, importantly, how the citizens were to be informed of their rights. Freese's high profile approach on this issue in particular was crucial in attracting public support and discouraging certain politicians and bureaucrats from challenging him. Moreover, like Simitis, he was something of a political fixer - comfortable operating in the corridors of power. In conclusion, Freese demonstrated 'the importance of personality and a capacity for public relations in trying to make data protection effective'[99]. This clearly strengthened the position of DIB and raised the profile of data protection in Sweden generally.

*Revision following Directive 95/46/EC*

In Sweden, the licensing approach had allowed DIB significant powers to stipulate specific conditions on collection, storage, manipulation and communication of personal data. For this reason, the supervisory agency's attitude towards the Directive was one of scepticism[100]. Seipel, a Swedish academic, argued in 1996 that there was: 'concern that the Directive reflect[ed] outdated – possibly even muddled – thinking on personal data protection'[101], and that it bought together in a piecemeal fashion bureaucratic elements from existing data protection laws that would prove very difficult to implement in national laws.

For Sweden, the Directive heralded a change in approach towards data protection. The 1973 Data Act, and its subsequent amendments, was concerned with files. This legal thinking dating from the early 1970's had been increasingly difficult to apply to the 1990's realities of databases and global data networks. The practicality had to be faced of providing a steady stream of information to data subjects about who is controlling which personal data. In this respect, a flexible attitude towards the Directive was recommended, with the mandate of the committee set up in Sweden to revise the 1973 Data Act indicating that it would be necessary to look for solutions which reflected national experiences and even rely on innovative methods[102].

Secondly, the Data Act 1973 did not cover manual processing. Indeed, the Data Act has been described as 'a typical computer privacy legislation'[103]. Thirdly, when the Data Protection Directive was first drafted in 1990, there was concern about its impact on the principle of free access to public documents guaranteed by the Swedish constitution. A number of provisions in the earlier drafts of the Directive (1990 and 1992) made it questionable to what extent this freedom of information provision could be maintained without conflicting with the principle of personal data according to the Directive. However, such a complex reconciliation was resolved in the final text following lobbying from the Swedish government. A clause - Recital 72 - was inserted into the preamble, augmenting the Articles of the Directive:

> 'this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive.'[104]

Thus, Recital 72 explicitly allowed for freedom of information within the framework of the Directive. This ensured that personal data could be legitimately processed, for example when 'necessary for compliance with a legal obligation to which the controller is subject'[105].

The Personal Data Act (PDA) 1998[106], in which Sweden implemented the Directive, came into effect in October 1998. It heralded some important changes to the Swedish culture of data protection regulation. Most significantly, the system of licensing and issuing permits was abolished. The Directorate-General of DIB described the change in his authority's role thus:

> 'Whereas formerly DIB was primarily a permits authority, PDA has now made it an authority increasingly concerned with supervision, counselling and information.'[107]

All data processing was instead to be notified to the supervisory authority, which maintained a record of the notifications. However, organisations were exempt from notification if they appointed a data representative and gave notice of this to DIB. This process of notification owed a little to the UK tradition of registration discussed in section 4.5.4, with the appointment of a data representative indicative of the German concept of a company 'privacy' officers.

Other key features included the extension of the scope of the Act to manual records and – four years prior to the Electronic Communications Directive - the requirement for controllers to seek the opt-in consent of the data subject prior to using personal data for direct marketing[108]. Finally, it was explicitly stated that the provisions of the new Act would not be applied to limit the principle of access to official documents. Indeed, provisions concerning freedom of the press and freedom of expression in the Freedom of the Press Act and Fundamental Law on the Freedom of Expression prevailed over the provisions in the PDA 1998[109].

### 4.4.3 Germany: federal data protection

The German data protection law built on those of Hesse (1970) and Rhineland-Palatinate (1974). A federal data protection bill was proposed in the mid-1970's to accompany another measure – the introduction of a national personal identification number to increase data processing efficiency[110]. Although, the latter provisions were rejected, the Federal Data Protection Act became law in

1977. The basic division of jurisdiction between the federal and the state data protection statutes was relatively straightforward. The Federal Data Protection Act covered data processing of personal information in the private and public sectors, but it was largely limited to regulating the public sector at the federal level. Land data protection laws primarily regulated the public sector at state levels, but there was a tendency towards special measures to regulate particular activities in the private sector, such as credit reporting. Private sector users were not supervised by the Federal Data Protection Commissioner, whose scope was restricted to registered federal users. Instead, they were regulated by various authorities (at state level) which had general oversight of private companies, for example, the authority which regulated banking had to ensure they complied in addition with various data protection rules. There was no general requirement for the private sector to register, setting the German data protection system apart from those in Sweden and, later, in the UK.

The Federal Data Protection Act was the first national law in Europe to attempt regulation of manual records. However, there were restrictions. For example, the information system (manual or automatic) had to demonstrate some of the sophisticated characteristics which computers can impart[111]. A further constraint was that manual data in the private sector processed for internal use could be excluded from all but one of the Act's provisions.

The statute was regulated in West Germany by the Federal Data Protection Commissioner. An intermediary between citizen and record keeper, the Commissioner relied on complaints from the citizens to identify trouble spots and launch investigations. The most important function of the Commissioner was the auditing of data processing. This required expert staff and powers to inspect premises, examine records and give advice and recommendations on the secure application of new technologies. The key problem was one of employing political resources: supportive political opinion; skilled and motivated staff; leadership; and access. Data protection was just one political interest among many, and its status as an issue depended on its position in the political agenda and the ability of the supervisory authorities to seize on favourable public and legislative opinion. In

the period up until the Census Decision in 1983 (discussed below), this proved particularly difficult.

As in Hesse, the Commissioner's powers were essentially advisory, although the Commissioner could compel government bodies to respond to his or her criticisms. Each public authority had to ensure compliance in its own field. Ultimately, the statute relied on the government to regulate its own data handling. Moreover, the Act had numerous exemptions. Section 13 declared that a federal body should not supply the data subject with information from his record where (among other circumstances) it would be 'to the disadvantage of the Federal Republic or of a Land (State)'; or where the data must be kept secret 'by the reason of their nature, in particular by reason of an overriding and justified interest of a third person'[112]. Simitis, the Hessian Data Protection Commissioner of the time, said of the German statute in 1977: 'In the history of the Federal Republic of Germany there may seldom have been an Act, to put it mildly, which contains so many reservations'[113].

However, it has been pointed out in defence of the Act, that it served as a foundation for more specific privacy measures, and that section 3 established a far-reaching principle that the processing of personal data is forbidden except where authorised by statute or by the consent of the data subject. The enforcement of the multi-tiered German data protection legislation was complex, comprising: administrative supervision at federal and state level; responsibility of designated corporate data protection officers in the private sector; and criminal offences for which fines and imprisonment may be imposed. These offences include failure to notify data subjects, failure to appoint a corporate data protection officer, and failure to give sufficient, correct, and timely information.

*The Census Decision*

A milestone in the German data protection debate was the Census Decision made by the Federal Supreme Constitutional Court 1983[114]. The federal government had planned a census which was of interest to many subsystems of public administration - for example, police, social insurances, resident's register – for

updating their records. A large number of questions were to be raised concerning living conditions, housing, commuting, family situation, work, leisure time behaviour and similar private interests. According to the dedicated Federal Census Act, each household was obliged to respond to these questions. However, it was not decided in the Act, which subsystem of public administration should get access to which data. The data matching potential was therefore considerable, as one agency in theory could have gained access to all data. This concern, coupled with the failure to prohibit people from officially collecting data in their own neighbourhood, resulted in public disputes and demonstrations[115].

On 15 December 1983, the Federal Supreme Constitutional Court held that the collection and processing of a vast amount of individualised census data was unlawful and infringed the Constitution[116]. The dignity of man (Article 1 (1) of the Constitution) and the right to personal freedom (Article 2 (2)) had been breached, if a person did not know who was processing what data on him for what purposes. The very general wording of this Decision ensured it extended beyond the census to impact on the private sector. Moreover, the Court ruled that, in particular, profiling a person was an offence against the Constitution. Following that decision, the 'right to informational self-determination' was deemed a part of personal liberty and personality. This latter point is significant as it presented a modern view on the pervasiveness of information processing and its impact on the private, individual sphere. The Court had recognised the informational self, and the individual's right to privacy and dignity in his exchanges in an information society. The federal data protection law had achieved general acceptance. As a result of this decision, millions of printed census questionnaires had to be destroyed[117].

The judgement was followed in Germany by a series of sector specific legislation, culminating in a revision of the general data protection law in 1990[118]. The burden of argument shifted to those who sought to limit privacy. Against the background of the Constitutional clarification of the right to determine the use of one's personal information, the 1990 Act now intended to 'protect the individual against his right to privacy being impaired through the handling of his personal data'[119]. For personal data to be handled, the person affected must agree to this, or there

must be a statutory arrangement. Moreover, whereas the 1977 Federal Act stated that data protection began with the existence of a file, the 1990 Act altered this so that data protection began with collection – the deliberate acquisition of personal information. In the private sector, however, the threshold at which data protection covered information remained that of a file. All details of persons held in other ways, for example, lists or books, were not covered by the Act. Finally, the existence of data protection agencies as necessary elements of data protection regimes was confirmed. This activist view to data protection – commencing with the privacy needs of the individual, rather than the processing requirements of data controllers – impacted on the Directive, although by 1995 many European countries had already established their specific understanding of data protection[120].

*Revision following Directive 95/46/EC*

The EU Data Protection Directive owed more to Germany's Federal Data Protection Acts (1977 and 1990) than any other national legislation. Like the Directive, Germany's federal data protection legislation had been based on the assumption that each processing operation on personal data involved an intrusion of privacy which demanded legitimation. The legitimation may be obtained by express legislation or by the informed consent of the person concerned. Two other principles gained fundamental importance: the idea of purpose-orientated data processing and the idea of anonymising personal data as far as possible.

In this context, a German academic, Kilian, stated that the Directive would result in a lowering of the German level of data protection[121]. In particular, concern was expressed at the permission given by the Directive for free flow of personal data between EU member states which have differing levels of protection[122]. This called into question which rights would remain for the German citizen in practice. The Directive was formally implemented through a series of amendments to the 1990 Federal Data Protection Act. The amendments entered into force in May 2001, and are a short-term measure whilst German data protection law undergoes a major review. This review is ongoing[123].

### 4.4.4 The Netherlands: codes of conduct

The Netherlands was cautious in its national approach towards data protection. Although bills had been published since the mid-1970's[124], the Data Protection Act (DPA) was not passed until 1988 – entering fully into force in 1990. The Act promoted self-regulation, and provided consumers with certain rights, including notice, access to information, disclosure and correction of inaccuracies. Both manual and computerised records were covered. The DPA required those in control of personal data files to take measures to assure only authorised disclosures and ensure informational accuracy. A data subject had to be informed of the collection of data within one month in writing. Notice had to contain the purpose of the file and the name and address of the file controller. Finally, the DPA allowed consumers to seek and obtain compensation for damages.

The Act created a Chamber of Registration, responsible for monitoring data protection development, advising the Dutch cabinet on relevant matters, and enforcing the provisions of the Act. Under the DPA, controllers of personal files containing data relating to more than one person were obliged to fill out a form (if private sector) or make a regulation (public sector), and send it to the Chamber in order to register.

However, the Dutch law has been most notable for introducing codes of conduct in their regime – an approach often cited, particularly during the 'Safe Harbor' negotiations. In consultation with the Chamber, professional organisations were able to adapt certain clauses in the law to their particular sector. By the beginning of 1996, approximately ten codes of conduct had been approved by the Chamber[125]. The law provided for a closely-knit connection between self-regulation and state supervision. Part of this model was adopted by the EU, with Article 27 of the general Directive incorporating codes of conduct:

> 'The member states and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by member states [...], taking account of the specific features of the various sectors.'[126]

At the time of adoption of the Directive, the impact of the DPA was under review as a matter of routine[127]. The findings of the evaluation, published in December 1995, recommended exploiting the Directive's potential for an optional procedure for the approval of codes of conduct[128].

The main difference between the Dutch DPA 1988 and the Directive was in scope. The latter was a new generation of legislation that replaced the static concept of 'personal data files' with the more dynamic concept of 'processing personal data'. The DPA had only applied in the former situation. As in a number of situations, processing of personal data will take place without the creation of a personal data file, the scope of the Directive was much wider.

Another point of interest was the provision in Article 18 (2) offering simplification or exemption from notification for controllers that appoint a personal data protection official in accordance with the national law. In the Netherlands, with the exception of a few municipal privacy committees, privacy officers per company were rare[129]. The German method of appointing such officers provided that the officer controlled the appliance of the national data protection law within the organisation – keeping a register of all the data processing and remaining independent as a consequence. Bergfeld argued that a combination of codes of conduct and privacy officers per branch or sector might lead to better results in the Netherlands than notification[130]. Overall, Bergfeld argued that the final text of the Directive was a sound basis for data protection in the Netherlands.

*Personal Data Protection Act 2000*

The Directive was implemented through the Personal Data Protection Act (PDPA) 2000[131], which entered into force in September 2001. At the same time, the Chamber of Registration was replaced by the Personal Data Protection Commission – marking the change in emphasis from concentrating solely on registration to overseeing the whole cycle of data processing. Indeed, the dated concept of 'personal data files' was replaced with 'processing of personal data', thus extending to the collection and acquisition of personal data. The previous

distinction between public and private sector was cancelled, with government institutions also having to notify their data processing operations with the new Commission. The concept of the organisational data protection official was introduced. Finally, codes of conduct remained prominent[132], with the supervisory authority able to declare that such codes properly implement the Act. Such declarations are valid for up to five years.

## 4.5 Data Protection in the UK: context

From the 1960's, data protection measures were being discussed in the UK. Concerns about new technological developments received increased attention in Parliament. A number of private members' Bills, some dealing with limited aspects of privacy and others with privacy as a whole, were introduced, although none reached the statute book[133]. The earliest privacy Bill was introduced in the House of Lords in 1961 'to protect a person from any unjustifiable publication relating to his private affairs and to give him rights in law in the event of any such publication'[134]. Further privacy Bills were introduced in the House of Commons in 1967[135] and 1969[136]. Additionally in 1969, Bills were introduced in both Houses concerning computerised personal information[137]. Finally, in 1972, another Bill was introduced to control both computerised and manually processed databanks[138]. However, it was not until the Data Protection Act 1998 – twenty six years later - that manually processed data was to be finally regulated in the UK.

To some extent, the new public concern was due to developments in information technology. Some government computers had been designed to facilitate the centralisation of information about people's private affairs and their dissemination for purposes other than those specified. Additionally, there had been a spectacular growth in the collection and distribution of information as a commercial activity, giving rise to anxiety in connection with granting of credit and mail order businesses[139].

## 4.5.1 Common Law and the Younger Report on Privacy 1972

The catalyst towards further government enquiry in this area proved to be the 1969 Right of Privacy Bill introduced by Brian Walden MP, and drafted by JUSTICE[140] – the British section of the International Commission of Jurists. Influenced by the conclusions of the Nordic Conference two years earlier, this Bill called for the creation of a general right of privacy, with civil remedy provided for certain infringements. However, in the course of its second reading debate in the House of Commons, the Labour Home Secretary James Callaghan announced that the government was to appoint an official Committee on Privacy in May 1970 with Kenneth Younger MP as chairman[141]. It was given the remit of considering whether legislation was needed to 'give further protection to the individual citizen and to commercial and industrial interests against intrusion into privacy by private persons and organisations'[142]. Thus, it was restricted to considering the private sector, plus the BBC and British universities.

The Committee paid detailed attention to the contemporary legal situation. There was no right to privacy as such in the law of England and Wales. Yet some aspects of privacy were already covered by existing law designed for other purposes – for example, trespass, nuisance, defamation and breach of confidence. Of those, the Committee considered the most effective protection to be the remedy in breach of confidence. This tort afforded a means of protection for all specific and reasonably implied confidences, except where the disclosure of the information given in confidence is shown to be in the public interest[143]. Indeed, the Committee believed the extent of this remedy's potential effectiveness was not as widely recognised as it should be. As such it was recommended that the law relating to breach of confidence should be referred to the Law Commission 'with a view to its clarification and statement in legislative form'[144].

In English law, there had not been a tradition of protecting the rights of citizens. Instead, reliance had been more on the principle that what is not prohibited is permitted. The main emphasis in civil rights, therefore, had been on keeping within acceptable limits, and providing precise definitions of the restrictions imposed by civil and criminal law on the individual's freedom of action. This

differed from Scotland, where the common law was to a considerable extent derived from the civil law, with a tendency to rely on general principles and readiness to assert general rights which it was the duty of the courts to uphold, exercising a wide interpretative discretion. In this way, Scotland was more in line with continental Europe which had general rights embodied in their written constitutions.

On the problem of definition – one of the obstacles to the development of a satisfactory law on privacy - the Committee concluded that the right to privacy had two main aspects. Firstly, a freedom from intrusion upon oneself, one's home, family and relationships. This was effectively the broad social value that privacy embodies – one that depended on the outlook of the individual - and it was questionable whether this would be suitably regulated on the basis of common law, slowly built up and tending to reflect the values of an earlier period rather than contemporary society. The second aspect defined by the Committee related to privacy of information. This definition essentially tackled data protection - the right to determine for oneself how, and to what extent, information about oneself should be communicated to others. In conclusion, Younger decided there was no need for a general privacy law. Rather, the Committee pointed to the adoption of specific proposals in the report, some of which related to the use of computers. On balance, it was deemed better to accept the remnant of difficult cases that may remain, than to attempt to deal with them all by means of a general privacy measure that may have a serious impact on other rights, in particular, freedom of communication[145].

The use of computing technology was taken seriously by Younger, with an entire section of the Report devoted to the collection and handling of personal information and its possible misuse in private sector[146]. The Committee stated that most of the problems which concerned them in this area were 'common to all data banks whether computerised or not'[147]. Chapter 20 of the Report concerned the use of computers for information storage and handling in the private sector. The Committee believed there was sufficient potential threat, and public and private disquiet, to justify serious attention being given to the establishment of appropriate safeguards. To this end, the Committee recommended ten guiding principles for

the use of computers that manipulated personal data[148]. Known as the Younger Principles, they were an important indication of the data protection principles that were to underpin both the 1984 and 1998 Acts:

(i) The purpose of holding data should be specified;
(ii) There should only be authorised access to data;
(iii) There should be minimum holdings of data for specified purposes;
(iv) Persons in statistical surveys should not be identified;
(v) Subject access to data should be given;
(vi) There should be security precautions for data;
(vii) There should be security procedures for personal data;
(viii) Data should only be held for limited relevant periods;
(ix) Data should be accurate and up to date;
(x) Any value judgements should be coded.

These principles concentrated mainly on security and access to data rather than dissemination of information. Communication between computers, for example in the form of data matching or, from the mid-1990's, the internet - had yet to become a significant feature of day to day computing. Younger recommended that these principles should form the basis of a voluntary code of practice which could be adopted by computer users[149]. The Report also proposed the setting up of a 'standing commission'[150] to consider the use of computers and their impact on individuals, in both public and private sectors.

### 4.5.2 White Paper: *Computers and Privacy* 1975

The government responded to the Younger recommendations concerning computers in the White Paper *Computers and Privacy*[151] (1975), in which it announced its intention to consider legislation. In parallel with the Younger Committee's enquiry into the private sector, the government had reviewed the categories of information held in the computer systems of government departments and the rules governing its storage and use. The results of that review, together with information concerning the rest of the public sector, were

also published in 1975 as *Computers: Safeguards for Privacy*[152]. This report found no evidence of improper use of computers in the public sector.

Nevertheless, the White Paper highlighted the need for regulation, stating that 'those who use computers to handle personal information...can no longer remain the sole judges of whether their own systems adequately safeguard personal privacy'[153]. The threat to privacy was identified as arising from five particular features of computer operations:

(i) They facilitate the maintenance of extensive record systems and retention of data in those systems;

(ii) They can make data easily and quickly accessible from many different points;

(iii) They make it possible for data to be transferred easily from one information system to another;

(iv) They make it possible for data to be combined in ways which might not otherwise be practicable;

(v) They store, process and often transmit data in a form which is not directly intelligible.

Importantly, point (iii) made reference to dissemination of information. With usage of the Internet almost universal in Western society, this has now become a major issue, over 25 years on from the publication of the White Paper.

The government, in *Computers and Privacy*, acted on Younger's recommendation of setting up a 'standing commission' concerning the processing of personal information with computers, by announcing the establishment of a Data Protection Committee. It was to seek to secure that all existing and future computer systems in which personal information was held – in both public and private sectors – were operated with appropriate safeguards for the privacy of the data subject. The government viewed the introduction of legislation as involving two key elements:

(i) The establishment of a set of objectives to set standards governing the use of computers that handle personal information;

(ii) The establishment of a permanent statutory agency to oversee the use of computers in both public and private sectors.

The ten Younger Principles recommended for the private sector were seen as an important base for the first element of the proposed legislation: 'the objectives to be declared in the statute should, therefore, cover very much the same ground.'[154] However, the influences behind the establishment of a statutory data protection agency were less clear. Nevertheless, the two models proposed - registration and licensing, or an ombudsman – suggested the government had at least had reference to the experiences of Sweden and Germany respectively, although it was yet to make up its mind about the best way forward[155].

### 4.5.3 The Lindop Report on Data Protection 1978

The Committee on Data Protection began work in July 1976, chaired by Sir Norman Lindop[156]. Membership comprised of six specialists in areas relevant to privacy and information technology, and six so-called "lay people", including the chairman himself. When interviewed for this thesis[157], Lindop stated that the two key experts were Paul Sieghart and Charles Read. Sieghart was a barrister, a human rights advocate and the primary author of the White Paper *Computers and Privacy*. He was involved in bringing together the members of the Committee other than the chairman. Read, director of the Inter-Bank Research Organisation, was "an excellent Committee man"[158].

In conducting its task, the Lindop Committee undertook several studies. Firstly, on the relationship between privacy and data protection, the Committee found that the function of data protection law should be different from that of privacy law. Rather than establishing rights, it should provide a framework for finding a balance between the interests of the individual, the data user (the processor of personal data) and the community at large.

Secondly, concerning the implications of technological progress, the Committee found that the proportion of all information processing activities conducted by

automatic means had increased, and would likely increase further[159]. Distinctions between manual and computerised systems had become increasingly blurred. As a result, the legislation had to be sufficiently flexible to 'enable the rules governing the handling of personal data to evolve over time'[160]. Thirdly, the Committee considered the public and private sector. This was the first large scale independent review into the use of personal data by both central and local government and the industrial and private sectors. Younger had only been permitted to survey the private sector. Yet, some public bodies proved reluctant to participate, with the secret services and the police particularly wary of the work of the Committee[161]. As a result, Lindop had to rely on the work of an investigative journalist Stewart Tendler regarding the Police National Computer[162]. The outcome from this multi-sector review was that data protection legislation needed to be flexible. A single set of rules to govern all handling of personal data by computers would not be sufficient. The legislation had to strike appropriate balances between all legitimate interests.

Lindop recommended that the scope of the legislation should extend to all automatic handling of personal data in the UK by any user, in both public and private sectors. The definition of 'automatic' was to be wide-ranging, including organisations where *any* part of the operation was conducted automatically. A set of seven statutory principles should be included to reflect the interests of the data subjects, users and communities at large. These covered broadly the same area as Younger, and in detail were[163]:

*In the interests of data subjects*

(i) Data subjects should know what personal data relating to them are handled, why those data are needed, how they will be used, who will use them, for what purpose, and for how long;

(ii) Personal data should be handled only to the extent and for the purposes made known when they are obtained, or subsequently authorised;

(iii) Personal data handled should be accurate and complete, and relevant and timely for the purpose for which they are used;

(iv) No more personal data should be handled than are necessary for the purposes made known or authorised;

(v) Data subjects should be able to verify compliance with these principles;

*In the interest of users*

(vi) Users should be able to handle personal data in the pursuit of their lawful interests or duties to the extent and for the purposes made known or authorised, without undue extra cost in money or other resources;

*In the interests of the community at large*

(vii) The community at large should enjoy any benefits, and be protected from any prejudice, which may flow from the handling of personal data.

The principles were not to be directly enforceable, but were to guide the actions of the supervisory authority. This body – the Data Protection Authority – was to implement the principles, ensuring that personal data was handled with adequate safeguards for the interests, in particular the privacy, of the data subjects.

Lindop recommended mandatory registration for computer users. Additionally, the Committee proposed the development and adoption of Codes of Practice to ensure compliance with the principles. Such codes would have the force of law, and any breach would be a criminal offence. Different codes would be prepared for different classes of personal data applications, in the same way codes have been drafted and developed for closed circuit television (CCTV) and employment data under the 1998 Data Protection Act. However, although this recommendation was not adopted in the UK for the DPA 1984, it did form the basis of the law passed by the Netherlands in 1988. The fact that there is a provision in the 1998 Act proved the concept to be an enduring one[164].

## 4.5.4 The UK Data Protection Act 1984

### *Processes*

Following publication of the Lindop Report in October 1978, progress towards data protection legislation was slow, with a general election in 1979 compounding the delay. The issue lacked a specific catalyst to bring it to the forefront of public debate. In the UK there had been no equivalent to the establishment of central population registers that had been proposed in many European states. Politically, the new Conservative government opposed the Lindop proposals – especially to the creation of another quasi-autonomous non-government organisation, or quango, in the form of the Data Protection Authority[165]. This perceived extra layer of bureaucracy was clearly set against Conservative pledges to yield substantial savings through the 'reduction of waste, bureaucracy and over-government' outlined in their 1979 general election manifesto[166]. However, the adoption by the Council of Europe of Convention 108 and the formulation of the OECD guidelines on transborder data flow reinforced concerns of many Conservative MPs that UK companies would be at a disadvantage when competing in the international data processing market[167]. In March 1981, the Home Secretary, William Whitelaw, announced the government's intention to legislate in order to ratify Convention 108. The latter treaty was signed by the UK in May 1981 (see Table 1, page 82).

However, the idea of an independent data protection authority was still contentious. Initially, the intention was to allow the Home Office to act as its own watchdog over public computers. In September 1981 the Home Office Minister of State, Tim Raison, referred to the call for an authority as 'fundamentally objectionable'[168]. In July 1981 Sir Norman Lindop, frustrated at the lack of progress, had reconvened the Data Protection Committee. Two papers were issued by the Committee members[169]. The members reiterated the arguments against conferring supervisory powers on government, the largest single user of personal data. They believed other European countries would doubt the credibility of data protection compliance in the UK if it was regulated by the Home Office. Under Article 12 of Convention 108, other countries could restrict transborder data traffic where the regulations of another country 'do not provide an equivalent protection'.

The members did point out that these tasks could be discharged by a single Commissioner with an adequate staff rather than the multi-member authority originally proposed.

By January 1982, the government – still adamant there should not be an independent authority - had moved towards the idea of an independent registrar[170]. At a conference in May 1983, Lindop stated that the reasoning for this shift was twofold, being:

> "...partly because the medical profession said they would not cooperate, but partly also because of the weight of evidence that the chief problems do lie in the public sector."[171]

In terms of timescale, the critical statement was made by Prime Minister Margaret Thatcher in a verbal reply during Prime Minister's Question Time, in February 1982, when the Labour MP Michael Meacher raised a question about the publication of his medical records on the front page of a daily newspaper. Thatcher commiserated with him, announcing it was the government's intention to legislate on data protection in the next Parliamentary session. As Lindop stated a year later:

> "I believe this was the first the Home Office knew about it; they were put rather smartly on the spot and had to produce a White Paper which bore all the signs of being cobbled together in a hurry."[172]

The White Paper, *Data Protection: the government's proposals for legislation*[173], was published two months later. It fell short of Lindop's recommendations, with the government deciding not to adopt legally enforceable codes of practice. Under the proposed legislation, the data protection authority would comprise a Registrar appointed by the Crown equipped with a staff of about twenty. The Registrar would be independent of the government but required to make an annual report to Parliament. All users of data systems in the public and private sectors who automatically process information relating to identifiable individuals would be

required to register. The Registrar would have powers to make inquiries, inspect data files, and require modifications to be made to a system or refuse registration.

Overall, the tone adopted in the paper was one of reluctance on the part of the government: 'the public sector costs and manpower will have to be contained within existing planned totals even if this means deferring application of legislation in this area'[174]. Clearly, commercial considerations had quickened the need for legislation – in particular, the need to ratify Convention 108 and so protect Britain's role as a 'crossroads on the international data highway'[175]. As the White Paper reflected, 'without legislation firms operating in the United Kingdom may be at a disadvantage compared with those based in countries which have data protection legislation'[176].

The first Data Protection Bill[177] introduced on 22 December 1982 was poorly received. Disappointment was expressed by groups as diverse as the British Medical Association, the National Computer Users' Forum, the Consumers' Association and Society of Conservative Lawyers[178]. Criticism centred on the omission of manual files and the sweeping exemptions from registration. Computers concerned with national security were fully exempt, whilst those concerned with tax, immigration, health, social work and crime detection and prevention were all partially exempt. A lead article in *The Times* captured most critics' perception of the Bill:

> 'Commerce, not liberty, is the motive power behind the government's legislation in the field of data protection. Fear of losing markets, not the desire to defend individual privacy against computer-driven intrusions, colours the clauses of the Data Protection Bill.'[179]

The first Bill fell with the dissolution of Parliament in May 1983, but a revived Bill – essentially similar – was introduced in July 1983. Although subject to much the same criticism as previously, it received Royal Assent on 12 July 1984 with minor amendments relating to compensation for inaccuracy and the exemptions from registration. The difficult passage of both Bills underscored the complexities inherent in the creation of an entirely new body of law ultimately based – via

Convention 108 – on fundamental rights which were recognised but undefined. Moreover, this highlighted the problems faced with constant opposition from bodies such as the Home Office, which viewed the data protection policy as an attack upon the traditional administrative control of personal information[180].

*Provisions*

The DPA 1984 required users to register automatically processed 'personal data' – information which related to a living individual who could be identified from the information, including any expression of opinion about the individual. The eight data protection principles were taken almost directly from the Council of Europe Convention 108. In addition to the establishment Office of the Data Protection Registrar (ODPR), a tribunal was created to hear appeals against the Registrar's sanctions by aggrieved data users. Although the registration system was borrowed from Sweden, it was the UK government – and not the Data Protection Registrar – that decided data protection policy as a whole.

However, the principles only applied to data which was registered. Accordingly, this had the effect that users who failed to register could not be required to comply with the principles[181]. Additionally, the legal provisions were slow to take effect – being phased in over a period in excess of three years from enactment of the DPA in July 1984. From September 1984, individuals damaged by the loss of data or its unauthorised disclosure could claim compensation in the courts. Registration was delayed until November 1985, and non-registration was not an offence before May 1986. Finally, subject access as well as the Registrar's supervisory powers did not become available until November 1987. This piecemeal implementation of the DPA was of benefit to users for whom data protection was new, but slowed application and enforcement of the law.

*Development of data protection law*

Although the government could look to laws in other countries when drafting the principles of data protection, the task of putting the legislation into practice was experimental. The ODPR had to gain the not only compliance, but also

understanding of a wide range of data users, many of whom had been hostile to the legislation. There were few obvious precedents. Raab[182] argued that implementing the DPA 1984 involved challenging powerful public and private sector interests dependent on the collection, processing, use and transfer of large amounts of personal data with a minimum of interference. The promotion of personal claims to privacy was set against the claims of efficient and effective public and private administration.

The fact that the DPA 1984 had been implemented to protect the interests of commerce rather than the consumer was in conflict with the approach taken by Younger and Lindop during the 1970's. Their reports had been fuelled by concerns over the loss of personal privacy in the computer age. Internationally, Convention 108 had been based on the right to private life in the ECHR. However, this point was omitted from the DPA 1984. Disregarding any questions of personal privacy, the long title of the 1984 Act was:

> 'An Act to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information.'[183]

This appeared to have the effect of removing individual privacy considerations from interpretation of the 1984 Act except with reference to Convention 108 – the provisions of which the DPA 1984 essentially made law. In the UK, Raab[184] argued, the ODPR actually had few allies available for support in enforcing individual privacy considerations. There were apparently few votes in data protection, public opinion was largely passive, and there were few civil liberties groups campaigning in this field. In a 1982 Mori poll, two thirds of those asked disagreed with the statement: "I am suspicious about the possible effects of new technology"[185]. Further, the choice of Eric Howe, a computer professional, as the first data protection Registrar reflected the more pragmatic motivation behind the Act and of the people implementing it.

However, in the early 1990's an important tribunal decision marked a move away from the purely technical approach to data protection[186]. It concerned the credit

reference industry's use of third party information. This had resulted in people being denied credit because of the bad debts of others who happened to live at the same address in the past. The Registrar viewed this as unfair processing, a breach of the first data protection principle. In 1991, the tribunal agreed with the ODPR, stating:

> 'It is quite clear...that the purpose of the Act is to protect the rights of the individual about whom data is obtained, stored, processed or supplied, rather than those of the data user.'[187]

Based on the evidence earlier in this subsection, the above statement was contentious. In the long title of the DPA 1984, there had been no suggestion that any special priority was to be given to the data subject. In its ruling, therefore, it could be argued that the tribunal was going beyond the intentions of the original UK legislation. However, the decision was more in line with Convention 108 and its concern with the protection of individual rights. The pronouncement thus represented a significant stage in the development of UK data protection law. It was evolving from purely a pragmatic technical statute, towards one recognising the privacy rights of individuals. At the same time, it was a signal of the increasing influence of the ODPR that, by the mid-1990's was tackling issues as diverse as identity cards, privacy at work, electronic government and cryptography[188]. The tribunal decision had strengthened the hand of the ODPR when advising and negotiating with users in those new fields of interest.

## 4.6 UK Data Protection Act 1998

### 4.6.1 Implementing a data protection infrastructure

The 1984 Act left the Data Protection Registrar with a huge administrative burden. There was uncertainty about the expected number of data users – in the first six months, there were 136 000; by 1994 this had only increased to 202 000. Elizabeth France, in her first annual report as Registrar (1995) believed the real number should have been around 500 000[189]. Raab[190] commented that whilst

during the first ten years of the DPA 1984 the infrastructures for implementation of data protection had been formed in the UK, they were fragile and existed along adversarial modes of conducting relationships. There was the need to balance competing interests of business, a reluctant government and the privacy of the individual.

During the 1990's there was a shift across Europe from computers, privacy and bureaucracy towards 'information'. Transactions were recorded and kept longer. Information was disseminated to more people in more remote locations at greater speeds. As people became less aware about what happened to their data, it became more easily accessible and manipulated, correlated and analysed in new ways not possible in days of the filing cabinet. Boundaries, particularly between public and private sector data, became blurred. It was into this context that the EU Data Protection Directive was passed in 1995. In the UK, the Directive was implemented as the DPA 1998.

### 4.6.2 Key provisions affecting information privacy

The DPA 1998 represented the first UK Data Protection legislation for fourteen years. Despite clear provisions in the 1995 Directive relating to private life, the UK legislation failed to make any reference to privacy. The long title of the DPA 1998 was:

> 'An Act to make new provision for the regulation of the processing of information relating to individuals, including obtaining, holding, use or disclosure of such information.'[191]

The DPA 1998 included significant changes from its predecessor in six key areas[192]:

(i) *Manual processing* – the 1998 Act applied to certain manual files in addition to automated data;

(ii) *Legitimacy of processing* – new conditions for processing existed as minimum threshold requirements before processing could be lawfully undertaken;

(iii) *Sensitive data* – a new category of personal data was created. Sensitive personal data could not be processed unless one of a set of certain pre-conditions was satisfied;

(iv) *Data transfer* – transfers of personal data to countries outside the European Economic Area[193] (EEA) were banned unless certain conditions were satisfied;

(v) *Data security* – data could not be processed unless processing complied with new security requirements;

(vi) *Individual rights* – significantly more and stronger rights for individuals existed under the new legislation including the right to compensation for damage or distress caused by unlawful processing.

These, in theory, strengthened the individual right to privacy. However, it is the final feature – individual rights – that the remainder of this sub-section will focus on, as they have most direct effect on the privacy of individuals.

Individual rights included the right to a description of:

(i) Personal data of which an individual was the subject;

(ii) Purposes for which the personal data are being processed;

(iii) Recipients or classes of recipients to whom personal data may be disclosed.

Additionally, the data subject is now entitled to have communicated to him in a form capable of being understood:

(i) Information constituting any personal data of which the individual is the data subject;

(ii) Any information available to the data controller as to the source of that data.

Furthermore, under the secondary legislation[194] a request for any of the above five pieces of information must be treated by the data controller as a request for all five. Other new rights included that in the cases of automated decisions, the logic of the decision be conveyed – for example, in credit scoring by a bank assessing the person's suitability for a loan. Additionally, data subjects have a right to stop data controllers processing data intended for direct marketing, or that would cause distress or damage to the data subject or a third party. An individual who suffered damage or distress due to contravention is entitled to compensation.

### 4.6.3 Key provisions affecting employees

An area of information handling that has received increased attention from regulators, lawyers and academics has been the processing of employee data. Moreover, the questionnaire survey and expert interviews in Chapter 6 highlighted that data controllers required further guidance concerning individual rights in this field. Consequently, this issue merits further discussion in order to provide context to the fieldwork findings. Personal data about employees includes name, address, date of birth, payroll details and CCTV images. Additionally, some sensitive data may be involved, for example, criminal convictions, physical and mental health data, and trade union membership. As the DPA 1998 covers such a significant area of work, commentators have recommended that all large and medium sized organisations put in place a data protection officer to ensure compliance[195]. The compliance officer should be effectively trained and be senior enough to have the authority to carry through the reforms. The reforms include: training staff; undertaking a thorough review of all personal data held by the employer; and setting up procedures and policies for governing relationships between employer and employees. For the bulk of organisations the key compliance date was 24 October 2001, when the provisions for processing manual data entered fully into force.

One of the many ambiguities with processing employee data has been the thorny issue of sensitive data. Schedule three of the DPA 1998 listed the pre-conditions under which such data may be processed. One of them was 'explicit consent' – a

concept yet to be tested in the courts - but which referred to unambiguous, freely-given consent. The most obvious way to obtain this would be in writing, for example in an employment contract. Additionally, employees must be informed of all purposes of such processing. To guarantee employee data security, the Personnel Policy Research Unit suggested employers comply with BS 7799[196] – the British Standards Institute standard concerning information security, and viewed by the Data Protection Commissioner as evidence of good records management.

Fundamentally, under the new Act, employees are entitled to gain access to personal data held by the employer. Job applicants are entitled to see any record of reasons for being refused the job applied for. Moreover, they must be informed that a decision has been taken by automated means. Section 56 criminalised enforced subject access – the process of employers forcing a data subject to make a subject access request in order to obtain records of, say, credit ratings or any criminal convictions. Finally, employees are entitled to compensation where employer processing caused unwarranted and substantial damage or unwarranted and substantial distress.

Another significant area concerns the transfer of employee data abroad. Under the eighth data protection principle, employers cannot generally transfer personnel files or names of job applicants outside of the EEA. In both cases, the recipient country will need ensure an 'adequate' level of data protection, as defined by Article 25 of Directive 95/46/EC[197], or have one of the exemptions listed in schedule four (for example, consent of the employee). Interestingly, transfers to third countries can proceed if specifically authorised by the member state's data protection commissioner. This has yet to happen in the UK. However, this did happen in Germany when an agreement was reached in 1996 allowing Citibank to transfer personal data from Germany to the US under German data protection law[198].

Finally, there has been considerable controversy in the UK over the issue of employee surveillance. Legitimate business reasons do exist for some surveillance – for example: if an employee is suspected of fraud; to monitor time spent surfing

the Internet; or to review emails for discrimination or defamation. In most cases, employee surveillance will amount to the processing of personal data. Under the first data protection principle, surveillance must be undertaken fairly and lawfully – requiring the consent of the employee, ideally in a contract of employment. The employee should be able to withdraw consent to any type of processing at any time. The fifth data protection principle stated that data be processed no longer than necessary, meaning that data obtained through surveillance should be destroyed or erased as soon as it is clear such data is not required for disciplinary or other action against the employee. Public sector employees also need to have regard to Article 8 of the ECHR – although where employees consent to surveillance, they can be taken to have waived their right to privacy.

*Codes of practice*

A new feature of the DPA 1998 has been the power for the Information Commission to establish codes of practice for 'guidance as to good practice'[199]. 'Good practice' is defined in section 51(9) of the Act as having regard to the interests of data subjects and others, and includes compliance with the requirements of the Act. According to the Commission's Annual Report 2000[200], the code of practice must provide 'added value'. To date (January 2003), codes of practice have been drafted in two areas: CCTV[201] and employment[202]. The former code was broadly welcomed. The code concerning employment – parts of which are still under consultation – was more controversial.

According to the Commission, two developments necessitated a code of practice in employment. Firstly, technology had widened the scope of processing of personal data. Decisions increasingly relied on processing personal data through, for example: with aptitude, psychometric, and even drug and genetic tests; scanning of application forms and CVs; interception of emails; and CCTV surveillance. The second development was the new legal environment with the DPA 1998 and the HRA 1998. This has generated significant public interest and concern.

The draft *Code*, published in October 2000, provided detailed standards on all aspects of employment: recruitment; employment records; access and disclosure; contract and agency staff; employee monitoring; medical testing; discipline and dismissal; and retention of records and former employees. Particular attention was given by the press to employee monitoring. Of significant note was the assertion that the more automated the processing, the more likely it was to be covered: 'systems that involve the interception of personal electronic communications such as email will almost certainly be covered'[203]. Specific business purposes should be established for monitoring, and such monitoring should be targeted. Employers should assess the impact on privacy, autonomy and other legitimate rights of staff. Staff should be aware it is taking place, and its purpose. The monitoring should be for limited purposes only. Employers were advised that information can be misleading or false. Detailed provisions were then provided on: covert monitoring; monitoring of communications such as telephone, email and Internet; on video and audio monitoring; and vehicle monitoring. Failure to comply could result in enforcement action by the Commissioner and a claim for compensation by the individual who has suffered as a result.

The Commissioner believed the *Code*, when finalised, would provide some certainty as to the requirements of the law and as to what is good practice. Employers were not obliged to adopt the *Code*. If compliance can be achieved through another method, the data controller was free to follow that. However, the *Code* will be of strong evidential value, providing a potent defence against actions under the Act by disgruntled employees or the Information Commission. In many instances there is probably only one set of practical possibilities. Finally, the code could be incorporated into human resource management, professional standards and management handbooks.

Publication of the draft *Code* generated considerable debate. As a result, the release of the final Code has been repeatedly delayed owing to extensive consultation and revision lasting over two years. The final Code is to be released in four parts. At the time of writing (January 2003), two parts have been finalised: *Part 1: Recruitment and selection* and *Part 2: Records management.* According to Assistant Information Commissioner, David Smith, *Part 3: Monitoring at work*

was due to be finalised "before Christmas" 2002 [204]. This timetable has slipped somewhat, raising questions as to whether the OIC will achieve its stated aim of completing *Part 4: Medical information* "before Easter" 2003[205].

The most vocal critic during the extensive consultation process has been the Confederation of British Industry (CBI), representing UK employers. The CBI voiced 'significant concerns'[206] about the draft, not least its length and complexity with over 200 standards set out in 62 pages. In April 2002, following the publication of Part 1, the CBI reiterated their position, complaining about the ad-hoc nature of the OIC's consultation process and stating that:

> 'The main premise of monitoring must be that business should be free to decide when and how to monitor employees at work, provided that employees are made aware of this. We have commented on the proposals but believe that they remain fundamentally flawed.'[207]

Trade unions, however, broadly welcomed the measure, stating that the OIC was correct in providing such detailed guidance. A representative from the Trades Union Congress (TUC) stated:

> "It is a hugely complicated area of law, and employers do need to put in place policy, and they need a clear simple guide which takes you through those policies [...]. There's no reason why an employer can't read a lot of documents if it's actually going to protect them from litigation in the future"[208].

The OIC has reiterated its position that the Code simply explained, and did not create, legal obligations[209].

## 4.7 North America

Article 25 (1) of the Data Protection Directive stated that the transfers of personal data could only take place to third countries[210] that had an 'adequate' level of data

protection. This posed particular problems for the US and Canada – both major trading areas for EU member states. The two countries have responded to the EU Directive and the potential threat of trade barriers in contrasting ways. The US, over a two year period, negotiated a set of principles for its companies to voluntarily sign up to – providing a 'Safe Harbor' for companies to continue to trade with the EU. However, the 'Safe Harbor' agreement has proved controversial, being opposed by many US businesses and the current US administration as presenting a barrier to free trade. Conversely, it has been contested by many within the EU – particularly the European Parliament - as not going far enough in protection personal data. Canada, with some tradition of data protection laws, extended its federal data privacy law to the entire private sector. This enhanced data protection regime, with limited exceptions, was formally recognised as 'adequate' by the EU in December 2001[211].

### 4.7.1 United States

*The Constitution versus common law*

Until the mid-1960's, privacy law in the US had largely developed via the courts. This had been achieved at two judicial levels. Firstly, the constitutional level at which the federal courts measured statutes against the rights enshrined in the US Constitution. Secondly, at common law level, by which judges fashioned remedies for particular invasions of privacy.

The US Constitution did not contain an explicit right to privacy. Indeed, the word privacy was not even mentioned. The closest guarantee was the fourth amendment, which held that:

> 'the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures shall not be violated'[212].

Therefore, the Supreme Court developed a doctrine known as 'substantive due process' that extended constitutional protection over some types of personal behaviour. This doctrine served as the basis for the constitutional right to privacy. The due process clauses in the fifth and fourteenth amendments barred the federal government and the states from depriving any person of life, liberty or property without due process of law. From the late nineteenth century, the Court began to use due process to protect certain substantive rights. This included a right to privacy from government surveillance into an area where a person had a 'reasonable expectation of privacy'[213] and also matters relating to marriage, procreation, child-rearing and education. The Court also recognised in *NAACP v. Alabama*[214] (1958) that political groups had the right to prevent disclosure of their members' names to government agencies. The idea was that people had the right to live their lives as they desired.

A key privacy decision taken by the Supreme Court was *Griswold v. Connecticut*[215] (1965) which struck down a state law prohibiting married couples from using contraceptives. There was no rational reason for such a law, the Court ruled, and it too drastically interfered with the basic intimacy of the marriage bond. Described by Westin in 1967 as 'a major first step towards enunciating a new constitutional doctrine of privacy'[216], it paved the way for a more controversial case. In 1973, the Court held in *Roe v. Wade*[217] that states cannot bar a woman from having an abortion because of the constitutional right to privacy. As it went against the deep convictions of many people, the case attracted huge political controversy. In spite of hearing many abortion cases in the years since *Roe* and changing the rules somewhat, the Court has declined to back away from the central point: that a woman has a constitutional right to control her body.

The development of a general common law right to privacy was first rationalised by Warren and Brandeis in a famous article in the *Harvard Law Review* in 1890[218]. They argued that the existing case law already contained the necessary ingredients to make up a general concept of privacy, but that the courts had not seen the wood for the trees. Judicial decisions had protected individual privacy under traditional headings of trespass, nuisance, slander, libel plus various property rights. Such incidental interests of privacy needed to be isolated from the existing remedies and

re-classified under a separate and independent liability of privacy. In this way, it would be possible to more clearly understand the concept involved and to protect privacy in a wider range of situations. This argument eventually became accepted in the US, and by 1960 there were over three hundred reported cases on the right to privacy[219].

In 1960, Prosser attempted to clarify the privacy case law and found not one law, but a complex of four torts[220]:

(i) Intrusions upon the plaintiff's[221] seclusion or solitude or into his private affairs;
(ii) Public disclosure of embarrassing private facts;
(iii) Publicity that places the plaintiff in a false light;
(iv) Appropriation for the defendant's[222] advantage of the plaintiff's name or likeness.[223]

According to Linowes and Bennett[224], it was the *Griswold v. Connecticut* case before the Supreme Court in 1965 that brought case law and constitutional law together - with the Supreme Court granting privacy constitutional status, as existing within the 'penumbras' of the Constitution[225]. Thus, the span and application of the concept of privacy widened.

In terms of public policy, privacy as a problem emerged with the development and spread of computer technology in the 1960s, especially with its application to government. Particularly important was the abortive attempt to establish a 'National Data Center' of all basic statistical data originating in federal agencies. The proposal floundered when scrutinised by Congress. Simultaneously, this was the period when privacy became regarded as more of a policy problem than something that can be protected in the face of rapid technological change by case law[226]. From that moment forward, 'informational privacy' or 'data protection' was distinguished from other behavioural aspects of privacy (such as physical intrusion), and granted its own separate distinction as an issue of public policy. The publication of important books by Miller[227] and Westin[228] during this period played a critical role in defining the problem.

*Freedom of Information Act 1966*

The federal legislature from the mid-1960's developed data protection law. The federal Freedom of Information Act (FOIA) 1966[229] was not primarily intended as a data protection measure, but did have the effect of improving government record-keeping. FOIA was designed to make executive records more accessible to the public. Nine categories of sensitive government data were exempt from disclosure, with appeals to the ordinary federal courts where the burden of proof was on the agency to justify its action in withholding any information. The exemption most relevant to data protection was for 'personnel and medical files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy'[230]. In the early days of FOIA, after it went into effect in 1967, there were bureaucratic attempts to refuse requests for access on the grounds that disclosure would be an unwarranted invasion of the applicant's privacy[231]. However, from the late 1960's increasing use was made of the FOI Act by individuals to ask for files compiled on them by federal security agencies.

Westin stressed that Congress was aware that the Act would provide a basis for safeguarding from disclosure private information about citizens that government has acquired, and that the citizen's right to privacy was a goal of the FOI Act along with the public's right to know[232]. The Act was a data protection measure in two senses: it provided a right of subject access to records – manual and automated – held by federal government; and it protected the privacy of third parties by exempting records from access if disclosure involved a 'clearly unwarranted invasion of privacy'[233]. Finally, there was one other exemption to the FOI Act which served to protect personal privacy: the exemption from disclosure of any information exempted by another statute. Following clarification by the Supreme Court[234], the main effect of this provision has been to protect from disclosure records such as tax returns and census information.

*Privacy Act 1974*

Privacy invasions in general had been a subject of Congressional interest since the mid-1960s, yet the idea of legislating a set of fair information principles to protect the right to information privacy was principally motivated by the long-term efforts of Senator Ervin. In the House of Representatives, a broad bipartisan agreement on the basic content of the law was fostered by the efforts of Congressmen Koch (Democrat, New York) and Goldwater (Republican, California). At the same time the privacy law was being debated, the FOIA was amended. That the Privacy Act[235] and the amended Freedom of Information Act became law at all was due to the significance of the events surrounding Watergate and the ensuing climate of distrust of government[236].

The US Privacy Act of 1974 differed from the European data protection laws in that the detailed rules were in the statute itself. There was no supervisory authority - rather the onus of enforcement mainly fell on the individual, who was to take legal action in the courts. The Act protected records held by federal government agencies, requiring them to apply basic fair information practices. Both manual and computerised files were regulated in this sector. The Act provided for a subject access right, but with exemptions to cover any records maintained by the Central Intelligence Agency and most records maintained by the Federal Bureau of Investigation. However, a right was established to request amendment of a record if it was not accurate, relevant, timely or complete. Finally, there was a right to damages if the data subject suffered harm from incorrect records, although this right required proof of some adverse effect of the erroneous information.

An important part of the Privacy Act was the creation of a temporary Privacy Protection Study Commission (PPSC). The establishment of this body was a compromise, after Senate moves to create a Federal Privacy Board – to have broad powers over both public and private sectors – were blocked[237]. The Commission examined individual privacy rights and record-keeping practices in many environments, including the private sector. When it reported in July 1977[238], the PPSC restated the 'eight privacy commandments' of openness, individual access,

correction and amendment, collection limitation, internal use limitation, disclosure limitation, information management, and accountability. Overall, the Privacy Study Commission assessed the Act to be only moderately successful[239]. It also found that, owing to the diversity of the subject matter, a single all-encompassing federal law would not be practicable. Instead, the PPSC made a series of recommendations to cover certain areas of the private sector, some legislative, others relying on voluntary compliance. The piecemeal legislation has been directed at particular practices and industries, and has included the Fair Credit Reporting Act 1970, Family Educational Rights and Privacy Act 1976, Right to Financial Privacy Act 1978, and the Computer Matching and Privacy Protection Act 1988. The Safe Harbor Principles, agreed in July 2000, and discussed later in this Chapter may broaden this approach to data privacy legislation.

The Privacy Act's greatest success was probably in establishing the extent and nature of personal record-keeping practice in federal government. In this, a supervisory role was assigned to the Office of Management and Budget (OMB), which was required to issue guidelines to federal agencies concerning implementation of the Act. Privacy Act officers were appointed in each agency. Standard operating procedures were instituted for the collection, use and dissemination of personal data. Additionally, there was a requirement on each agency to publish full details of its records systems in the federal Register and to give advance notice to Congress and the OMB of every new system of records and every major change in existing systems. This was in order to evaluate their privacy implications. Essentially, this constituted a limited form of registration, in spite of the generally different approach to privacy taken by the US in most other respects. In this capacity, the Act has contributed to the reduction of unnecessary information collection, in the elimination of a large amount of information from existing systems, and in the consolidation of a number of duplicate record-keeping systems. The Act has thus been described as a 'records management statute' rather than a mechanism to protect individual rights[240]. Indeed, Rule criticised the Act for concentrating on efficiency of record-keeping without critically evaluating the need for personal data systems in the first place[241].

*A 'Safe Harbor'?*

Historically, the US has taken a sectoral approach towards privacy protection – resulting in a patchwork of federal laws, state laws and self-regulatory programmes. There was no wish to enact a generally applicable data protection law on the lines of the EU Directive for its private sector. The resulting differences in approach threatened trade between the two powers. The EU is by far the US's largest trading partner and the site of most US foreign investment. In 2000, the US exported $255 billion of goods and services to the EU and imported $302 billion of goods and services from the EU[242]. Clearly, many US companies depend on information flows with suppliers, customers, partners, affiliates and other service providers based in the EU. Within the EU, the same is true. Any restriction on transatlantic data flows would matter to both partners.

*Provisions*

Therefore, the 'Safe Harbor' framework was developed by the U.S. Department of Commerce, in consultation with the European Commission, industry and non-governmental organizations. Under 'Safe Harbor', U.S. organisations could voluntarily adhere to a set of data protection principles recognised by the Commission as providing adequate protection. This arrangement was expressed in a set of seven privacy principles, augmented by 15 frequently asked questions and answers (FAQs)[243]. The FAQs are sector specific measures, detailing issues such as exceptions for journalists (FAQ 2); human resources data (FAQ 9); and the handling of publicly available information (FAQ 15).

US companies can receive personal data from the EU by means other than 'Safe Harbor'. For example, if data subjects have given their consent or the transfer is necessary to fulfil a contract involving the data subject[244]. Additionally, transfers can take place between two companies where the importer can guarantee that adequate safeguards are in place - for example, by contract[245]. These transfers required authorisation by the member states' data protection commissioners. However, the processed was simplified in December 2001 by the introduction of model contracts by the European Commission for exchanging personal data

between EU nations and third countries[246]. Under these voluntary contracts, EU companies exporting data would instruct the subcontractor to treat the data with full respect to EU data protection requirements and guarantee that appropriate technical and security measures are in place in the destination country. Member states' data protection commissioners are obliged to recognise that these transfers enjoy adequate protection.

The documents underpinning 'Safe Harbor' are extensive. They include the European Commission's adequacy decision (July 2000)[247] and the exchange of letters between the US Department of Commerce (DOC) and the European Commission[248]. These papers revealed the detail and complexity of the negotiations. The 'Safe Harbor' framework was finally agreed between the European Commission and the DOC in July 2000 after over two years of intense negotiations, and criticism from the European Parliament[249]. The framework, and its principles, came into force on 1 November 2000. The principles required the following:

(i) *Notice*. Organisations must notify individuals about the purposes for which they collect and use information about them;

(ii) *Choice*. Individuals must be given the opportunity to opt out if their data will be disclosed to a third party. For sensitive data, an opportunity to opt in must be given if the information is to be disclosed to a third party;

(iii) *Onward Transfer*. The notice and choice principles must be followed if disclosing information to a third party;

(iv) *Access*. Individuals must have access to personal information about them held by an organisation and be able to correct, amend or delete information where it is inaccurate;

(v) *Security*. Reasonable precautions must be taken to protect personal information from loss, misuse and unauthorised access, disclosure, alteration and destruction;

(vi) *Data Integrity*. Personal data should be accurate, complete and current;

(vii) *Enforcement*. There must be:

a. Readily available and affordable independent recourse mechanisms;
b. Procedures verifying that the commitments companies make to the 'Safe Harbor' principles are implemented;
c. Obligations to remedy problems arising out of failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organisation.

Companies were not obliged to show that they conform to the 'Safe Harbor' principles before they sign up. However, the principles had to be applied to any data transferred from the EU after the US organisation had entered the 'Safe Harbor'. Yet, there is no obligation to apply the principles to manually processed operations. Any organisation that wishes to extend 'Safe Harbor' benefits to human resources personal data transferred from the EU, has to indicate this when signing up to the principles and conform to the requirements set forward in FAQ 9[250].

*Enforcement*

Enforcement of the 'Safe Harbor' primarily takes place in the US, in accordance with US law. The method is largely through alternative dispute resolution mechanisms, whereby independent private sector bodies will investigate and attempt to resolve complaints in the first instance. If the companies fail to comply with the rulings of these bodies, the cases will be notified to the Federal Trade Commission (FTC) or the Department of Transportation, depending on the sector, which have legal powers to oblige them to comply. Serious cases of non-compliance can result in companies being struck off the DOC's list – ensuring they will no longer be able to receive data transfers from the EU under the 'Safe Harbor' arrangement. Additionally, under the FTC Act[251], a company's failure to abide by commitments to implement 'Safe Harbor' principles is likely to be considered a deceptive act likely to mislead reasonable customers in a material way. In such cases, the FTC has powers to impose heavy fines and require the payment of compensation to individuals. Such action would additionally produce

bad publicity and could trigger a stream of private legal actions. Thus, the FTC supports the private sector programmes.

For the US, the main motive behind the 'Safe Harbor' agreement was clearly economic. The DOC, on its dedicated website, has been keen to promote the benefits to business from entering 'Safe Harbor'[252]:

- All 15 EU member states are bound by the European Commission's finding on adequacy;
- Companies participating in 'Safe Harbor' are deemed adequate and personal data flows to those companies shall continue;
- Member state requirements for prior approval of data transfers is either waived or approval is automatically granted;
- Claims brought by EU citizens against US companies will be heard in the US subject to limited exceptions.

Essentially, the framework offers a simpler and cheaper means of complying with the adequacy requirements of the Directive than seeking approval from individual member states. An EU organisation can ensure it is sending data to a 'Safe Harbor' company by viewing the public list of 'Safe Harbor' organisations - posted on the DOC's website[253]. An organisation's appearance on the list constitutes a representation to the DOC and the public that it adheres to a privacy policy meeting the 'Safe Harbor' framework. By mid-January 2003, 292 US organisations – including Hewlett Packard, Dun and Bradstreet, and Microsoft - had signed up to the arrangement.

Following an initial implementation period, the 'Safe Harbor' agreement became fully effective from 1 July 2001. A European Commission working paper assessed the effectiveness of the agreement in February 2002[254]. The findings were mixed. Whilst acknowledging that all the elements of 'Safe Harbor' were in place, a substantial number of the US organisations that had signed up to the agreement were not observing the expected degree of transparency. This was regarding both their overall commitment and the contents of their privacy policies, less than half of which reflected all seven 'Safe Harbor' principles. This lack of

transparency risked the credibility of the whole arrangement. The paper also drew attention to the alternative dispute resolution mechanisms. Not all of the six private sector bodies elected to fulfil this task have publicly indicated their intention to enforce 'Safe Harbor', and not all had put in privacy practices applicable to themselves that conformed to the principles. Given this situation, the European Commission stated that only those mechanisms fully conforming to 'Safe Harbor' should be used by the 'Safe Harbor' organisations. A full evaluation of 'Safe Harbor' is planned by the European Commission during 2003.

Ultimately, the EU retains powers to intervene in certain cases, for example, to suspend data transfers to a US company disputing violations of the principles with the FTC. Additionally, if evidence of non-compliance accumulates and the relevant US enforcement body is dilatory or complacent - and if letting transfers continue risks causing grave harm to data subjects - EU authorities can again suspend transfers. The Commission can reverse its decision to grant the 'Safe Harbor' arrangement 'adequate protection' status.

*Reaction*

During the first half of 2001, reaction to the Data Protection Directive and 'Safe Harbor' in particular was hostile. Presidential elections held in November 2000 had replaced the Democrat administration that had agreed to 'Safe Harbor' with a more protectionist Republican government under Bush. In May 2001, *Ft.com* reported on a deepening dispute between the EU and the US over the Data Protection Directive[255]. The Bush administration had written to the Commission protesting against the model contract that financial institutions would be asked to sign to ensure that their exports to non-EU countries complied with the Directive. *The Independent* online had earlier highlighted the potential disruption to EU trade with the US if the 'Safe Harbor' agreement was to be dismantled – with companies having to seek permission of individual customers before their data can be transferred to the US[256].

However, following the terrorist attacks in the US on 11 September 2001, 'Safe Harbor' has become less of a concern for the Bush administration. The US

government did request in November 2001 that the EU revised its draft E-Communications Directive to permit the retention of data for a 'reasonable period', beyond what was necessary for billing purposes[257]. As discussed in sub-section 4.3.4 of this Chapter, such a revision was passed during the Directive's second reading before the European Parliament in May 2002. Thus, law enforcement agencies were granted greater access to electronic communications data. Finally, the earlier introduction of model contracts in December 2001 simplified the transfer of personal data between the EU and third countries, providing organisations with an alternative to 'Safe Harbor' when transferring personal data to the US[258]. Nevertheless, US business groups such as the Global Privacy Alliance – whose membership include Oracle, IBM and VeriSign – were still lobbying the European Commission to relax its data protection regime in autumn 2002[259].

### 4.7.2 Canada

Canada's development of data protection law was more typical of Western European countries, especially Germany. Early legislation in this field was at a state level, for example British Columbia enacted the Personal Information Reporting Act in 1973. During this period the federal government set up a Task Force on Privacy and Computers which published a number of independent studies and a summary report[260]. Following the report, the federal government set up an Interdepartmental Committee on Privacy in order to prepare a law for the federal government[261]. The outcome was the Human Rights Act of 1977: Part IV of which was entitled 'Protection of Personal Information'. The Canadian Human Rights Act only effected the public sector, but did regulate manual processing.

Regulation was by the Privacy Commissioner – essentially an advisory institution, as in Germany. However, the main powers were invested elsewhere - in this case, in a designated government minister. The statute ultimately relied on the government to regulate its own data handling. For example, sections 53-55 of the Human Rights Act enabled each Minister to exempt personal records kept by his own department from the data subject's right of access. For this reason, it came in

for some criticism at the time[262]. Additionally, although the various criteria for exemption were set out in the Act (for example, protection of national security, criminal intelligence, supervision of convicted persons), each Minister interpreted them for himself or herself.

Concrete proposals for amending Part IV, and creating a separate Privacy Act, were first put forward in 1980. In 1982, the Privacy Act[263] was enacted in tandem with an Access to Information Act. Both Acts were proclaimed in force on 1 July 1983. The federal Privacy Act provided individuals with a right of access to personal information held by the federal public sector. Seventeen years later, the Personal Information Protection and Electronic Documents Act[264] (known as Bill C-6) was passed by federal government - regulating how private sector organisations may collect, use or disclose personal information in the course of commercial activities. This measure came into effect on 1 January 2001, although its provisions are being phased in over three years. Both Acts are overseen by the Privacy Commissioner of Canada, who is authorised to receive and investigate complaints.

*The Privacy Act 1982*

The Privacy Act was Canada's first dedicated privacy legislation. It imposed obligations on federal government departments and agencies to respect privacy rights of Canadians by limiting the collection, use and disclosure of personal information. Data subjects were given a right to access and correct personal information held about them by federal government organisation. Moreover, the Act established a fair information code to regulate government handling of personal records. The code required the federal government to:

- Limit its collection of personal information to the minimum required to operate programmes or activities;
- Collect information, whenever possible, directly from the data subject;
- Inform the data subject why the information is being collected and how it will be used;

- Not use information for purposes other than those specified, unless allowed by law;
- Keep information for long enough to allow the person a reasonable opportunity to obtain access;
- Ensure information is as accurate, up to date and complete as possible;
- Not disclose personal information unless specifically allowed by the Privacy Act or another law.

Clearly, the code was not as specific as the data protection principles found in most national data protection laws in Europe at the time. Indeed, the code's provisions could be ignored when another federal act allowed for the processing of personal information. 'Personal information' was defined as 'any factual or subjective information, recorded or not, about an identifiable individual'[265]. However, personal information did not include a data subject's job title, telephone number or address, details appearing on an individual's business card, or that could be found through a publicly available source such as a telephone directory. The Privacy Act applied to a range of federal government records, including: pension and unemployment insurance files; medical records; tax records; and student loan applications. As the information may be recorded 'in any form', it included video and audio tapes, plus any electronic information medium.

However, from the late 1980's the federal government was under pressure to review and expand the provisions of the Act[266]. Due to growing commercial trade in customer information, the issue of data protection in the private sector became more prominent. In the mid-1980's self-regulation based on OECD guidelines had been encouraged. Industries such as insurance, direct marketing and telecommunications all drafted sector-specific codes. These codes were updated and harmonised in the mid-1990's by the Canadian Standards Association, resulting in the 1996 Model Code for the Protection of Personal Information[267]. In terms of statutes, Quebec became the first North American jurisdiction to adopt comprehensive legislation for information held by the private sector. In 1994, the province passed an *Act Respecting the Protection of Personal Information in the Private Sector*[268]. This Act granted individuals a right of access to personal information held by private sector businesses operating in Quebec and regulates

the collection, use and disclosure of personal information. Moreover, by January 2002, all but two provinces – Prince Edward Island and Newfoundland - had data protection legislation governing the collection, use and disclosure of personal information held by government agencies[269].

However, the coming into force of the EU Data Protection Directive with its 'adequacy' test on the transfer of data to third countries, prompted the federal government to enact legislation to control the use of personal data in the private sector.

*The Personal Information Protection and Electronic Documents Act 2000*

The Personal Information Protection and Electronic Documents Act (PIPEDA) built on the existing attempts to encourage self-regulation and will eventually regulate the entire private sector, filling some very important gaps in the patchwork of federal and provincial statutes passed over the last thirty years.

The Act is being implemented in three stages. Commencing 1 January 2001, the law applied to:

- Federal works, undertakings or businesses. It applied to personal information of clients and employees in the federally regulated private sector, such as airlines, banking, broadcasting, inter-provincial transportation and telecommunications;
- Personal information disclosed across provincial borders – and outside Canada - for consideration.

On 1 January 2002, the law was extended to personal health information collected, used and disclosed by organisations described under phase one of the law. Finally, on 1 January 2004, the Act will apply to:

- The collection, use and disclosure of personal information by any organisation in the course of commercial activity within a province;

- All personal information in all interprovincial and international transactions by all organisations subject to the Act in the course of commercial activities.

The federal government may exempt organisations and/or activities in provinces that have adopted substantially similar legislation. Provincial governments are therefore given the opportunity to pass their own statutes, or to do nothing and surrender an important constitutional power to the federal government in three years time when the entire private sector will be covered.

PIPEDA gave individuals a right to know why an organisation would collect, use or disclose their personal data; to do so reasonably and appropriately; and not to use the information for any purpose other than that to which the individuals have consented. Moreover, the data subject can expect to know who in the organisation is responsible for protecting their data and expect the organisation to take appropriate security measures. Consumers can expect the information held to be accurate, complete and up to date; to obtain access to their personal information and ask for corrections; and make complaints, in confidence if necessary.

Furthermore, organisations should destroy, erase or make anonymous personal information that it no longer needs in order to fulfil the purpose for which it was collected. However, there are exceptions to the above principles. For example, an organisation may not need to obtain consent if the information clearly benefits the individual and cannot be obtained in a timely way; or if the information is required by a law enforcement agency for an investigation.

In the new Act, sensitive data as such is not identified. Data is regarded as sensitive depending on the context in which it is used. There is no prohibition on the collection of such data, although it is recommended that an organisation 'should' generally seek express consent when the information is likely to be considered sensitive[270]. Finally, the Act stated that more sensitive data should be guarded by a higher level of protection[271].

Oversight of this legislation has been given centrally to the Canadian Office of the Privacy Commissioner. It is a complaints-driven, ombudsman model with powers to investigate complaints, call witnesses, compel evidence and inspect business premises. Organisations' practices can be audited on 'reasonable grounds' and the findings made public. Finally, the Commissioner's mandate includes research, education and the promotion of privacy issues in Canada[272]. However, the Commissioner has no binding powers and must apply to the federal court for enforcement. Nevertheless, it is a criminal offence to obstruct the Commissioner during an investigation or audit, or to knowingly dispose of personal information that could be subject to a request. Additionally, the legislation makes it a criminal offence for employers to take retaliatory actions against employees who blow the whistle.

In December 2001, the European Commission recognised the adequacy of PIPEDA[273]. In effect, the Commission's 'Decision' permitted the free flow of personal data from the EU to Canada subject to PIPEDA 2001 – covering private sector organisations that collected, used or disclosed personal information in the course of their commercial activities. The Decision did not, therefore concern data held by the public sector at federal or state levels, or private sector data held for non-commercial purposes, for example, employment data or personal information held by charities. Those transfers had to be conducted by other means, for example through model contracts.

However, since the terrorist attacks of 11 September, Canada has been under pressure from the US to amend its domestic legislation to increase security. Legislation has been passed restricting rights of access to personal information under both the Privacy Act and PIPEDA. The Attorney General has been given powers under the Canadian Anti-Terrorism Act 2001 (section 104) to prohibit disclosure of personal information for the purposes of 'protecting international relations or national defence or security'[274]. Furthermore, an amendment to the Aeronautics Act[275] overrode section 5 of PIPEDA by allowing foreign governments access to passenger lists on flights coming into, or departing from, Canada. Bennett[276] argued that the prime reason for these changes to Canadian data protection legislation were the 'significant pressures to converge with

dominant American practices'. The events of September 11 'convinced many American policy makers that American security was only as strong as that of the largest undefended border in the world'[277].

## 4.8 Conclusions

Data protection law is complex – evolving, overlapping with other legislation and diversifying into new fields. It is subject to pressures from government, business and the consumer. Moreover, with increased dissemination of personal data via stand-alone computers rather than centralised government databanks, data protection law needed to evolve. As a result, two generations of statutes have been passed in many European Union member states in 30 years. Indeed, Sweden and Germany have recently enacted third generation statutes. In the midst of this rapid progress, this Chapter has identified a few important, and overlapping, trends.

(i) Globalisation and the changing role of data protection laws

Over a period of three decades, legislation in this field has moved from national laws motivated by domestic concerns to international instruments such as the Council of Europe's Convention 108, the OECD's guidelines and the EU Data Protection Directive. Within Europe, early data protection laws in states such as Hesse, Sweden and Germany focused on the role of the computer – especially in public administration. This resulted in legislation (in the aforementioned states) or detailed recommendations such those in the UK's Lindop Report. In Canada, legislation was enacted covering the public sector, combined with the self-regulatory Canadian Standards Association's Model Code.

The enactment of Directive 95/46/EC represented a shifting in gears within the EU. Initially intended for information privacy and harmonisation, its focus altered during drafting to accommodate free trade - ensuring the transfer of personal data between member states, thereby benefiting the single market. Within its jurisdiction, the Directive has become a facilitator of free trade. In this respect, the

instrument had a global effect with its effective prohibition of the transfer of personal data to states lacking 'adequate' protection. Consequently, nations as diverse as Switzerland, Hungary and Canada have amended their data protection legislation to accommodate the provisions of the Directive. The US entered into the 'Safe Harbor' agreement with the EU. However, opposition to this agreement by the Bush administration – even prior to the attacks of 11th September 2001 – indicated that there are limits to the globalisation of data protection legislation.

(ii) The question of harmonisation within the EU – how far-reaching?

The Directive was enacted only after substantial structural changes within the European Communities – in particular the Schengen provisions concerning the sharing of information on criminals across borders, and economic moves towards the single market. Unlike the Council of Europe's Convention 108, the Directive is an all-encompassing piece of legislation that had to be transposed into law of member states. This meant that not only the UK, but also states such as Sweden with revised legislation, had to overhaul their national data protection laws – including manual records for the first time. In France and Ireland, this process is ongoing.

However, the effect will be far-reaching as the Directive absorbed different national approaches. Codes of practice were adopted from the Netherlands, the appointment of corporate data protection officers borrowed from Germany, and registration of data controllers adapted from the UK. Nevertheless exemptions, transition periods and flexibility exist. There has been room for individual states and organisations to develop their own best practices in relation to the Directive. In conclusion, this attempts to ease the tension between the 'convergence' and 'divergence' concepts postulated by Bennett in 1992[278].

(iii) Move towards a sectoral data protection legal environment.

In certain respects, Directive 95/46/EC has resulted a more flexible regulatory environment. Provision exists within the Directive (Article 27) for individual states to develop their own specific codes of practice. This provision has been

used by the OIC in the UK to develop codes of practice concerning usage of CCTV and processing of personal data in employment practices. Sector-specific codes of practice and the development of model contracts between organisations trading in different countries have become increasingly prevalent, with information privacy being viewed as a quality standard to be 'built-in' to good business practice. This observation will be developed further in the case study analysis (Chapter 7).

Finally, this trend towards specialisation was evidenced in the enactment two years later of the Telecommunications Data Protection Directive, superseded in 2002 by the E-Communications Directive.

(iv) Difficulties encountered by the UK supervisory authority in promoting new data protection practices

Nationally, the DPA 1998 has prompted UK organisations to revise their data handling practices, with new provisions concerning the management of personal information in manual records, wider individual rights, the introduction of more rigorous standards for handling sensitive data and the outlawing of enforced subject access requests. Organisational change will be analysed in more detail in the fieldwork Chapters – 6 and 7. Whereas the previous DPA 1984 focused on the handling of narrowly defined computerised data – being more of a records management statute – the DPA 1998 has its roots firmly in the European Convention of Human Rights, although the UK Act did not acknowledge this. In this respect, individual privacy – at least in the handling of individual's personal information – is key.

However, the UK supervisory authority has encountered difficulties in promoting certain new practices. In particular, the new provision concerning codes of practice has proved controversial. Whilst the OIC is insistent that such codes are merely mechanisms to aid compliance with the law, businesses have been concerned that they may be used set new standards of practice over and above the provisions of the DPA 1998. This has resulted in extensive delays in finalising the

Employment Practices Code of Practice. Moreover, it became clear during fieldwork interviews that the OIC was hampered resource and staffing problems – resulting in a backlog of work. A positive outcome of this was that local authorities at least, were more likely to approach each other with queries than the supervisory authority, resulting in greater networking among organisations. This debate is considered in further detail in the Chapters 6 and 7 detailing expert and case study interviews.

(v) Anti-terrorism amendments: 'convergence' at the instigation of the US?

Following the terrorist attacks in the US, most developed countries have been amending their domestic legislation. Both the EU and Canada have altered data protection legislation in response to US security concerns. The EU revised its draft E-Communications Directive to extend the retention of personal data, allowing law enforcement agencies greater access, whilst Canada amended PIPEDA, restricting data subject access and allowing foreign governments access to airline passenger lists. As Bennett[279] recently observed, US pressures are causing data protection policy– in a small way – to 'converge'. Whether this impact will be lasting, remains to be seen.

The above trends, overlapping and in some respects contradictory, nevertheless give an indication of the current legal situation regarding data protection. Issues such as moves towards sectoral codes and the difficulties encountered by the UK supervisory authority will be analysed further in the following Chapters. More specifically, the impact of other legislation, for example freedom of information concerns, on data protection laws will be discussed in Chapter 5.

## References and Notes

[1] Bennett, C.J. *Regulating privacy: data protection and public policy in Europe and the United States*, 1992. Some of the themes in this book were discussed in Chapter 3 (section 3.1.2).

[2] By 'sectoral', it is meant the application of guidelines – some binding, others voluntary – to various sectors of industry, such as banking and direct marketing. Usually, such guidelines are drawn up by industry bodies themselves, rather than imposed centrally by government.

[3] European Communities. Commission. DG Internal Market. *Data protection: Commission recognises adequacy of Canadian regime.* Brussels. 14/01/02. Refer URL: http://europa.eu.int/comm/internal_market/en/dataprot/news/02_46.htm (Accessed 16/01/03).

[4] This definition was later elaborated in a famous article by the lawyers Warren and Brandeis:

- Warren, S.D. and L.D. Brandeis. The right to privacy. *Harvard Law Review*, 4, 1890, 193-220.

[5] For Nordic Conference list of the 10 rights, refer:

- Great Britain. Committee on Privacy. *Report of the Committee on Privacy.* Chairman Kenneth Younger. HMSO, 1972. (Cmnd 5012), Appendix K, p.327.

[6] The Calcutt Committee on Privacy and Related Matters was set up in 1989 to consider what measures might be needed to protect individual privacy for the activities of the press. Its report in June 1990 resulted in a strengthening of the Press Complaints Commission. Refer:

- Great Britain. Home Office. *Report of the Committee on Privacy and related matters.* Chairman David Calcutt. HMSO, 1990 (Cm 1102).

[7] Article 8 of the ECHR states: 'Everyone has the right to respect for his private and family life, his home and his correspondence.' This definition on privacy will be discussed in greater detail in Chapter 5.

[8] Jay, R. and A. Hamiliton. *Data Protection: law and practice*, 1999, p.1.

[9] Raab, C.D. Police cooperation: the prospects for privacy. *In*: M. Anderson and M. de Boer (eds). *Policing Across National Boundaries*, 1994, pp. 124-5

[10] *Ibid.*

[11] Great Britain. Home Office. *Report of the Committee on Data Protection.* Chairman Sir Norman Lindop. HMSO, 1978. (Cmnd 7341), p.10

[12] It became known as the Nordic Conference of International Jurists on the Right of Privacy, Stockholm 1967.

[13] For further details, see the ICJ website: http://www.icj.org (Accessed 16/01/03).

[14] For the text of Brian Walden's Bill (26 November 1969) refer to *Report of the Committee on Privacy*, ref.5., pp. 276-8.

[15] The term 'data user' referred to organisations processing personal data. In Directive 95/46/EC, this was replaced by 'data controller'.

[16] Council of Europe. *Convention for the protection of Human Rights and Fundamental Freedoms.* Article 8. ETS no. 005. Rome, 1950. For full text, see URL: http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm (Accessed 16/01/03).

[17] Council of Europe. *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector.* Adopted 26/09/73. Explanatory Report, paragraph 2.

[18] *Ibid.*

[19] *Ibid.*, Annex.
The ten principles included standards that information should be: accurate; appropriate and relevant to purposes for which it is stored; not be obtained fraudulently; kept for specified periods; not be used for purposes other than those specified. Additional principles covered: the data subject's right to know about information stored about him; security of data banks; and the anonymising of statistical data.

[20] Council of Europe. *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector.* Adopted 20/09/74.

[21] *Ibid.*, Explanatory Report, paragraph 13.
Otherwise, the principles covered the same types of processing as Resolution (73) 22.

[22] *Resolution (73) 22*, paragraph 10.

[23] *Ibid.*, paragraph 9.

[24] Great Britain. Home Office. *Computers and Privacy.* HMSO, 1975. (Cmnd 6353), pp.9-10.

[25] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, ETS no. 108. Strasbourg, 1981. Explanatory report, paragraph 13.

[26] The two other terms of reference were:

> 'to carry out a study on data bank regulations, particularly for medical data banks;
> to examine problems relating to the professional ethics of computer experts.'

Refer:

- *Report of the Committee on Data Protection*, ref. 11. p.32.

[27] The explanatory report to the Convention stated that the instrument was titled as 'Convention', rather than 'European Convention': 'in order to better underline that there ought to be ample scope for accession to it by non-European states'. Refer:

- Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,* ref. 25, paragraph 24.

[28] *Ibid.*, paragraph 19.

[29] The explanatory report to *Resolution 73 (22)* made particular reference to the legislation in Hesse and Sweden. See ref. 17.

[30] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,* ref. 16, Article 12 (2).

[31] *Ibid.*, Article 4. This stated that the principles 'shall be taken at the latest at the time of entry into force of this convention in respect of that Party.' This is to avoid a legal vacuum between the date of entry into force of the Convention and the date on which domestic measures take effect.

[32] On this point, commentators appear to agree. Refer to, for example:

(a) Mellors, C. and D. Pollitt. Legislating for privacy: data protection in Western Europe. *Parliamentary Affairs*, 1984, 37 (2), pp.199-215.

(b) Carey, P. *Data protection in the UK*, 2000, p.2.

(c) Napier, B. Data protection begins to bite. *New Law Journal*, 141, 1991, p.497-498.

(d) Pounder, C. The data protection problem. *Management Today*, 1985, pp. 39, 43, and 46.

[33] For further details refer *Report of the Committee on Data Protection*, ref. 11, p34.

[34] Burkert, H. Privacy-data protection: a German/European perspective. *Second symposium of the German American Academic Council's Project 'Global Networks and Local Values'*, Woods Hole, Massachusetts, 3-5 June 1999 p.51. URL: http://www.mpp-rdg.mpg.de/woodsh.html [Accessed 16/01/03].

[35] Privacy Exchange. *Transborder personal data flows: administrative practice.* URL: http://www.privacyexchange.org/tbdi/pdataflow.html [Accessed 16/01/03].

[36] *Report of the Committee on Data Protection*, ref.11, p.34.

[37] Organisation for Economic Cooperation and Development. *Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data.* Adopted 23/09/80.

[38] *Ibid.*, section 19.

[39] Canadian Standards Association (CSA). 1996. *Model Code for the Protection of Personal Information.* CAN/CSA-Q830-96.

[40] This activity resulted in a 'Ministerial Declaration on the Protection of Privacy on Global Networks' in 1998. This stated that the 1980 OECD Guidelines were still sound but needed to be implemented, urging the private sector to apply them particularly in the context of global networks. Refer:

- Organisation for Economic Cooperation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2001. pp. 59-62. URL: http://www1.oecd.org/publications/e-book/9302011E.PDF (Accessed 07/05/03).

[41] The European Parliament's powers were extended in stages throughout the following two decades, with the first direct elections held in 1979. The Maastricht Treaty on European Union, when it came into force in November 1993, was the most significant force for change. It gave Parliament the right to approve the appointment of each new European Commission, and become more closely involved in the legislative process due to the complex co-decision procedure introduced by Article 189b.

[42] Mellors, C. and D. Pollitt, ref. 32(a), pp.204-205.

[43] *Ibid.*, p.204.

[44] European Communities. Commission. *Recommendation on Implementation of Convention 108 on the Automated Processing of Personal Data.* Official Journal of the European Communities. No. L246/31. (1981).

[45] European Communities. Commission. *Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.* Official Journal of the European Communities. No. L281/31. (23/11/95).

[46] European Communities. Commission. *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.* Official Journal of the European Communities. No. L024/01. (30/01/98).

[47] Table 2, p. 94, shows the 10 countries that had ratified Convention 108 by the end of 1990. Of these, the 7 EC countries: France, Spain, Germany, UK, Luxembourg, Denmark and Ireland. Sweden and Austria joined the EU, as it became after the Treaty of Maastricht, (along with Finland) on 1 January 1995. Norway is not a member of the EU.

[48] Bennett, C.J. ref. 1, pp. 7-8. The countries studied were: the US, Germany, the UK and Sweden.

[49] European Communities. Commission. *Data Protection: Background Information*, 1998. For full text, see URL: http://europa.eu.int/comm/internal_market/en/dataprot/backinfo/info.htm [Accessed 16/01/03].

[50] Burkert, H. ref. 34, p. 53.

[51] Raab, C.D. and C.J. Bennett. Protecting privacy across borders: European policies and prospects, *Public Administration*, 1994, 72, 95-112.

[52] By 19 December 1996, the Schengen area extended to all European Union member states with the exception of the UK and Ireland. In May 2000, the UK began to participate in the SIS. For EU information on all aspects of Schengen, refer URL: http://europa.eu.int/scadplus/leg/en/lvb/l33020.htm [Accessed 16/01/03].

[53] Council of Europe. *Recommendation No.R (87) 15 regulating the use of personal data in the police sector*. Strasbourg. Adopted 17/09/87.

[54] The eight were France, Germany, Belgium, the Netherlands, Luxembourg, Denmark, Ireland and the UK.

[55] The Schengen area came into effect in 1995. It abolished internal borders of signatory states and created a single external border where immigration checks for the Schengen area were carried out in accordance with a single set of rules.

[56] European Communities. Commission. *Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data.* Official Journal of the European Communities. (24/09/90). COM 1990 (0314).

[57] For a fuller analysis of the background to the Directive, and the reasons for the change in emphasis between the first and second drafts, refer:

- Pearce, G. and N. Plattern. Achieving personal data protection in the European Union. *Journal of Common Market Studies*, 1998, 36 (4), pp.529-547.

[58] European Communities. Commission. *Amended proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data.* Official Journal of the European Communities. (15/10/92). COM 1992 (0422).

[59] European Communities. *Treaty on European Union.* Maastricht, 1992. For full text, refer: http://europa.eu.int/en/record/mt/top.html [Accessed 16/01/03].

[60] The difference, therefore, between the European Union and European Community is slight. The Union is the overarching body, whilst the Community is responsible for implementing key policy elements such as economic and monetary union; single market; structural policy and the customs union.

[61] For full texts of both treaties, refer to URL: http://europa.eu.int/abc/treaties_en.htm [Accessed 16/01/03].

[62] Borchardt, K-D. *The ABC of Community law*, 2000, p.78.

[63] For details, refer to *The Amsterdam Treaty: a comprehensive guide.* URL: http://europa.eu.int/scadplus/leg/en/lvb/a10000.htm#a10007 [Accessed 16/01/03].

[64] Carey, P. ref. 32(b), p. 4.

[65] *Directive 95/46/EC*, ref.45, Article 1 (2).

[66] Jay, R. and A. Hamilton., ref. 8, p. 10.

[67] *Directive 95/46/EC*, ref.45, Article 7.

[68] *Ibid.*, Article 8 (1).

[69] *Ibid.*, Article 8 (2) (e).

[70] *Ibid.*, Article 30 (1).

[71] Kosten, F. and C. Pounder. The EC Data Protection Directive 1995: An analysis. *Web Journal of Current Legal Issues*, 1996 (2). URL: http://webjcli.ncl.ac.uk/1996/issue2/kosten2.html [Accessed 16/01/03].

[72] Carlin, F.M. The Data Protection Directive: the introduction of common privacy standards. *European Law Review.* 1996, 21(1), p.65-70.

[73] Blume, P. The citizens' data protection, *Journal of Information, Law and Technology.* 1998, 1. URL: http://elj.warwick.ac.uk/jilt/infosoc/98_1blum/blume.htm [Accessed 16/01/03].

[74] Rule, J.B. *Private lives and public surveillance*, 1973.

[75] Raab, C.D. and C.J. Bennett. Taking the measure of privacy: can data protection be evaluated? *International Review of Administrative Sciences*, 1996, 62 (4), pp. 535-556.

[76] Raab, C.D. *et al. Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: test of the method on several categories of transfer.* Final report. September 1998. DG XV.

[77] *Directive 95/46/EC*, ref.45, recital 10.

[78] Article 33 stated that the Directive was to be reviewed no later that three years following implementation. The delayed review is now underway. Part of the process involves two online surveys – one aimed at business and one at private individuals. The consultation exercise culminated in a conference on the implementation of Directive 95/46/EC in Brussels on 30 September – 1 October 2002. Refer: http://europa.eu.int/comm/internal_market/en/dataprot/2002-conf/index.htm [Accessed 16/01/03].

[79] Refer:

- European Communities. Commission. *Implementation of Directive 95/46/EC.* URL: http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm [Accessed 16/01/03].

[80] European Communities. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.* Official Journal of the European Communities. No. L201/37. (31/07/02).

[81] Article 2 (h) of the Electronic Communications Directive defines email as 'any text, voice, sound or image message sent over a public communications network' which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient. According to some commentators, this definition is wide enough to cover text messaging on mobile phones (SMS). The wording of Recital 40 appears to support this view. For further detailed analysis of Directive 2002/58/EC:

- Middleton, R. and D. Callaghan. European facelift for E-communications data privacy. *Privacy and Data Protection*, 2002, 2(7), 3-6.

[82] Cookies are small text files placed on the users' hard drive by the web server. They are used to store information about the user. The uses to which this information is put by various websites is the subject of much debate. For further information, refer URL: http://www.cookiecentral.com [Accessed 16/01/03].

[83] Refer:

- Grossman, W. A new blow to our privacy. *The Guardian*, 06/06/02. URL: http://www.guardian.co.uk/Archive/Article/0,4273,4427430,00.html [Accessed 16/01/03].

[84] *Ibid.*

[85] EurActiv.com. EP plenary adopts e-communications Directive. *EurActiv.com*, 31/05/02. URL: http://www.euractiv.com [Accessed 16/01/03].

[86] The information on the Council of Europe's Data Protection website has been updated to reflect changes in national laws since the enactment of Directive 95/46/EC. For further details, refer: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/ [Accessed 03/12/02].

[87] Bennett, C.J. Regulating the computer: comparing policy instruments in Europe and the US. *European Journal of Political Research.* 1988, 16 (5), 437-466.

[88] Michael, J. *Privacy and Human Rights*, 1994, p.95.

[89] In the constitutional system of West Germany following the Second World War, a new emphasis had been put on the executive and rule-making powers of the local communities, which carried the main burden of executing state and federal laws, as well as their local by-laws.

For further commentary, refer to: Burkert, H., ref. 34.

[90] Federal Republic of Germany. Land Hessen. *Data Protection Act of 7 October 1970.* For translation refer:

- Sieghart, P. *Privacy and computers*, 1976, pp. 160-164.

[91] *Report of the Committee on Data Protection*, ref.11, p.29.

[92] The importance of individual data protection commissioners, particularly during the first generation of data protection legislation, was emphasised by Flaherty:

- Flaherty, D. *Protecting privacy in surveillance societies*, 1989.

[93] Burkert, H., ref. 34, p.46.

[94] The Hesse Act and many subsequent German laws sought to avoid this 'state association' by making the agency or commission directly responsible to Parliament.

[95] Refer to:

- Banisar, D. Freedom of information and access to government records around the world. *Privacy International*, 2002. URL: http://www.freedominfo.org/survey/ [Accessed 16/01/03].

[96] For a translation refer to:

- Sieghart, P., ref. 90, pp. 165-171.

[97] Great Britain. *Report of the Committee on Data Protection*, ref.11, p.23.

[98] Flaherty, D., ref. 92, p.126

[99] *Ibid.*, p.128

[100] Seipel, P. Comments on the EC Data Protection, the view from Sweden. *The Journal of Information, Law and Technology*, 1996, 1. URL: http://elj.warwick.ac.uk/jilt/DP/1sweden/default.htm [Accessed 16/01/03].

[101] *Ibid.*

[102] *Ibid.*

[103] *Ibid.*

[104] *Directive 95/46/EC*, ref.45, Recital 72.

[105] *Ibid.*, Article 7 (c).

[106] Sweden. *Personal Data Act 1998*, Swedish Code of Statutes, SFS 1998: 204.

[107] Sweden. Data Inspection Board. *Annual Report 1999*. Stockholm: Data Inspection Board, 1999, p.4. Refer URL: http://www.datainspektionen.se/in_english/ [Accessed 17/07/02].

[108] Sweden. *Personal Data Act 1998.*, ref. 106, section 11.

[109] *Ibid.*, sections 7 and 8.

[110] Michael, J., ref. 88, p.95.

[111] The German Act used the definition of 'databank' to regulate its manual records. One of the features of such a databank was that 'it should not include files and collections of files unless they can be rearranged and evaluated by automatic means'. For further discussion, refer:

- *Report of the Committee on Data Protection*, ref.11, p.25.

[112] *Ibid.*, p.28.

[113] *Ibid.*

[114] Federal Republic of Germany. *Decision of the Federal German Constitutional Court*, Volume 65 (1983), 1ff.

[115] University of Strathclyde. ENLIST project. *Data Protection and Privacy – Commentary.* Section 5.3. URL: http://itlaw.law.strath.ac.uk/ENLIST/subjects/dpp/commentary/ [Accessed 16/01/03].

[116] *Decision of the Federal German Constitutional Court*,ref. 114.

[117] University of Strathclyde, ref. 115, Section 5.3. The decision had been preceded by an injunction in April 1983 by which the Constitutional Court stopped the census just two weeks before it was due to begin.

[118] Germany. *Federal Data Protection Act.* 20 December 1990. Federal law Gazette I 1990, p. 2954 with amendments.

[119] *Ibid.*, Part I, section 1 (1).

[120] See Burkert, H., ref. 34, p.55. The title of the French Data Protection Act 1978, already presented the core of the value programme: 'Informatique et *Libertés*' – informatics and freedom rights, meant that privacy was viewed as an overarching right to other rights and liberties.

[121] Refer:

- Wiebe, A. Harmonisation of data protection law in Europe. Report on the working conference on EC Data Protection Directive. *The Journal of Information, Law and Technology*, 1996, 3. URL: http://elj.warwick.ac.uk/jilt/confs/3dp/default.htm [Accessed 16/01/03].

[122] *Directive 95/46/EC*, ref. 45, Article 1 (2).

[123] Refer to website of the German Federal Data Protection Commissioner, URL: http://www.bfd.bund.de/information/engl_corner.html [Accessed 16/01/03]

[124] Refer:

- *Report of the Committee on Data Protection.*, ref.11, p.21.

[125] Bergfeld, J.P. EC Data Protection Directive, impact on Dutch data protection law. *The Journal of Information, Law and Technology*, 1996 1.
URL: http://elj.warwick.ac.uk/jilt/dp/1dutch/default.htm [Accessed 16/01/03].

[126] *Directive 95/46/EC*, ref.41, Article 27 (1).

[127] Bergfeld, J.P., ref. 125. It is not unusual in the Netherlands for legislation to be evaluated every five years.

[128] *Ibid.*

[129] *Ibid.*

[130] *Ibid.*

[131] The Netherlands. *Personal Data Protection Act 2000.* O.J. 302/2000.

[132] *Ibid.*, Articles 25 and 26.

[133] In total, six Bills were introduced in both Houses in the eleven years from 1961 to 1972.

[134] Lord Mancroft's Bill (14 February 1961).

[135] Alexander Lyon's Bill (8 February 1967).

[136] Brian Walden's Bill (26 November 1967).

[137] Kenneth Baker's Bill (6 May 1969); Lord Windlesham's Bill (26 June 1969).

[138] Leslie Huckfield's Bill (8 February 1972).

[139] The Younger Committee undertook a survey of public attitudes to privacy. For an example of public perceptions to computers, refer:

- *Report of the Committee on Privacy*, ref. 5, pp. 177-178.

[140] Refer:

- Great Britain. *Report of the Committee on Data Protection*, ref.11, pp. 276-278.

[141] The Younger Committee was formally appointed by the Labour Home Secretary, James Callaghan, on 13 May 1970. Following the change of government after the June 1970 general election, the Committee continued its work under the Conservative Home Secretary, Reginald Maudling. Its terms of reference remained unchanged.

[142] *Report of the Committee on Privacy*, ref. 5, p.1.

[143] *Ibid.*, p.26. A high profile example of the use of this case was in *Argyll v Argyll* (1967) where the Duke of Argyll was restrained from disclosing marital confidences – with a view to publication – entrusted to him by the Duchess during their marriage.

[144] *Ibid.*, p.16.

[145] *Ibid.*, pp.11-12.

[146] *Ibid.*, Part II, section B, pp. 72-115.

[147] *Ibid.*, p.72.

[148] *Ibid.*, p.183-184. According to Seighart, these were the first concise and comprehensive set of such principles to be published anywhere in the world. Refer: Sieghart, P. ref. 80, p.128.

[149] *Report of the Committee on Privacy*, ref. 14, p.16.

[150] *Ibid.*, pp.191-192.

In particular, the Standing Commission should review the ten principles 'to determine their relevance and adequacy in a changing situation and consider the case for giving them legislative force'. Additionally, it could receive complaints from users of computerised databanks and make recommendations for further controls for safeguarding the handling of their personal information.

[151] *Computers and Privacy*, ref. 24.

[152] Great Britain. Home Office. *Computers: Safeguards for Privacy.* HMSO, 1975. (Cmnd 6354).

[153] *Computers and Privacy*, ref. 24, p.8.

[154] *Ibid.*, p.9.

[155] *Ibid.*, p.11.

[156] The Labour Home Secretary Roy Jenkins announced the government's intention to appoint the Data Protection Committee in December 1975. It was originally to be chaired by Kenneth Younger, chairman of the Privacy Committee. However, his sudden death in May 1976 resulted in the appointment of Sir Norman Lindop, Director of Hatfield Polytechnic, in his place.

[157] For a full analysis of this interview, refer to Appendix A.

[158] Interview with Sir Norman Lindop, chairman of the Data Protection Committee 1976-1978. Hertford, 06/09/02.

[159] *Report of the Committee on Data Protection*, ref.11, pp. 13-18.

[160] *Ibid.*, p.xix.

[161] Refer to Appendix for further discussion.

[162] Refer:

- Tendler, S. Yard's new computer to hold 1.3 million criminal files. *The Times*, 14/02/77, p.2;
- Tendler, S. Special branch to put suspects' names on computer file. *The Times*, 09/09/77, p.1.

[163] *Ibid.*, p.290.

[164] Following the enactment of the EU Data Protection Directive 1995, codes of practice have increasingly become viewed as a pragmatic means of underpinning national data protection laws. Moreover, in counties with a cultural antipathy to overarching government legislation, such as the US, such codes are viewed as a practical alternative.

[165] Crook, A. Data protection in the United Kingdom, part 2. *Journal of information Science.* 1983, 7 (2), 55.

[166] Conservative party. *1979 general election manifesto.* Section 2: Restoring the balance. URL: http://www.psr.keele.ac.uk/area/uk/man/con79.htm [Accessed 16/01/03].

[167] In November 1979, John Butcher MP suggested to the Home Office that he should introduce a Private Member's Bill based on the Lindop recommendations which the government could help along without affecting its own programme. His suggestion was not taken up.

[168] Veitch, A. Data protection under fire from all sides. *The Guardian,* 16/09/81, p.2.

[169] The two papers were:

(i) Data Protection Committee members. *Memorandum submitted to the Home Office on data protection legislation for the UK*, July 1981. [Unpublished];

(ii) Data Protection Committee members. *Comments on the White Paper on data protection*, June 1982. [Unpublished].

[170] Crook, A. ref. 165, p.50.

[171] Lindop, N. Data protection: the background. *In*: C. Bourne and J. Benyon (eds). *Data protection: perspectives on information privacy*, 1983, p. 26.

[172] *Ibid.*

[173] Great Britain. Home Office. *Data protection: the Government's proposals for legislation.* HMSO, 1982. (Cmnd 8539).

[174] *Ibid.*, p. 7.

[175] *Ibid.*

[176] *Ibid.*, p.2.

[177] Great Britain. House of Lords. *Data Protection Bill.* 51. Session 1982-1983.

[178] Mellors, C. and D. Pollitt, ref. 32(a), p.210.

[179] The Times. Leader: Liberty takes a back seat. *The Times.* 12/02/83, p.9.

[180] Bennett's analysis stated that this was the reason for settling on a registration system as a compromise between the Swedish approach of licensing and Home Office control originally championed by Raison. Refer:

- Bennett, C.J., ref. 87.

[181] Jay, R. and A. Hamilton, ref. 8, p. 8.

[182] Raab, C.D. Implementing data protection in Britain, *International Review of Administrative Sciences*, 1996, 62 (4), p. 498.

[183] Great Britain. *Data Protection Act 1984.* London: HMSO.

[184] Raab, C.D., ref. 182, p. 498.

[185] Information Technology and People. Privacy, freedom and the Data Protection Act. *Information Technology and People.* 1983, 3 (6) 154.

This lack of public concern for data protection is mentioned by Timothy Raison in an interview:

> "I've represented my constituency for twelve years, and I've never had a single constituent come to me with any problem or question about data protection. It just doesn't feature in the ordinary person's imagination."

Quoted in:

- Riley, T. UK minister discusses data protection proposals: interview with Rt Hon. Timothy Raison, Minister of State for the Home Office. *Transnational Data Report.* 1982, 5 (8), 380-382.

[186] *CCN Systems Ltd v The Data Protection Registrar*, 1991; *CCN Credit Systems Ltd v The Data Protection Registrar*, 1991. For further analysis, refer:

- Napier, B. Data protection begins to bite. *New Law Journal*, 1991, 141, p.498.

[187] *Ibid.*

[188] Great Britain. Office of the Data Protection Commissioner. *First annual report*, 2000, pp.100-116.

[189] Great Britain, Data Protection Registrar. *Eleventh annual report*, 1995.

[190] Raab, C.D., ref. 183, 493-511.

[191] Great Britain. *Data Protection Act 1998*. London: HMSO.

[192] Identified by Carey, P., ref. 32(b), pp.6-7.

[193] The European Economic Area is the fifteen EU member states plus Iceland, Liechenstein, and Norway.

[194] Great Britain. Home Office. *The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000, No. 191.*

[195] For a detailed description of the processes involved in ensuring compliance at an organisational level, refer:

- Aiken, O. Statutes of liberty. *People Management*, 1999, 5 (12), 48-52.

[196] The British Standard for *Information Security Management*. For further details, refer URL: http://www.bsi-global.com/Business+Solutions/Infosec/index.xalter [Accessed 16/01/03].

[197] So far, only the data protection regimes in Switzerland, Hungary and Canada have met with EU approval.

[198] This related to an agreement between the German subsidiary of Citibank (Citicorp Deutschland AG) and the German national railway (Deutsche Bahn AG) to offer a combined rail discount card and Citibank VISA card. Citibank planned to process application forms in the United States. Following objections from data protection commissioners in three northern German states, an 'Inter-territorial Agreement' in 1996 was signed by the relevant Citibank entities - agreeing to abide by German data protection laws when processing the data.

Refer:

- Privacy Exchange. *Transborder dataflow*. URL: http://www.privacyexchange.org/tbdi/pdataflow.html [Accessed 16/01/03];
- Dix, A. The German railway card: A model contractual solution of the 'adequate level of protection' issue? *18th Privacy and Data Protection Conference*, Ottawa, Canada. 18-20 September 1996. URL: http://www.datenschutz-berlin.de/sonstige/konferen/ottawa/alex3.htm [Accessed 16/01/03].

[199] *Data Protection Act 1998*, ref. 191, section 51(3).

[200] Office of the Data Protection Commissioner. *First Annual Report*, ref. 188.

[201] Great Britain. Office of the Data Protection Commissioner. *CCTV Code of Practice*, 2000.

[202] Great Britain. Office of the Data Protection Commissioner. *Draft Code of Practice: The use of personal data in employer/employee relationships*, 2000.

[203] *Ibid.*, p.26.

[204] Smith, D. Assistant Information Commissioner. Data Protection: the Employment Practices Code. *NADPO annual conference*, University of Warwick. 18-19 November 2002.

[205] *Ibid.*

[206] Confederation of British Industry. *CBI response to the UK Data Protection Commissioner's Draft Code of Practice regarding use of personal data in employer/employee relationships*, 2001. [Unpublished].

[207] Confederation of British Industry. *Issue statement. Data protection: Employment practices code*, 2002. [Unpublished].

[208] Interview with Hannah Reed, Employment Rights Officer, TUC. London, 18/10/01.

[209] Eaglesham, J. Industry accused of blocking data act talks. *FT.com*, 14/05/02. URL: http://news.ft.com [Accessed 16/01/03].

[210] Countries outside of the European Economic Area (EEA) where the Directive is not directly applicable. See ref. 193.

[211] European Communities. Commission. *Commission Decision 2002/2/EC of 20.12.2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act.* Official Journal of the European Communities. No. L2/13. (04.01.2002).

[212] United States. *The United States Constitution.* 4th Amendment. URL: http://www.house.gov/Constitution/Amend.html [Accessed 16/01/03].

[213] United States Supreme Court. *Katz v. US*, 386 US 954 (1967). URL: http://laws.findlaw.com/us/386/954.html [Accessed 16/01/03].

[214] United States Supreme Court. *NAACP v. Alabama*, 357 US 449 (1958). URL: http://laws.findlaw.com/US/357/449.html [Accessed 16/01/03].

[215] United States Supreme Court. *Griswold v. Connecticut*, 381 US 479 (1965). URL: http://laws.findlaw.com/us/381/479.html [Accessed 16/01/03].

[216] Westin, A.F. *Privacy and freedom*, 1967, p.353.

[217] United States Supreme Court. *Roe v. Wade*, 410 US 113 (1973). URL: http://laws.findlaw.com/us/410/113.html [Accessed 16/01/03].

[218] Warren, S. and L.D. Brandeis, ref.4.

[219] Dworkin, G. Privacy and the law. *In*: J.B. Young, (ed.) *Privacy*, 1978, pp.113-136.

[220] A wrongful act, or infringement of a right (other than under contract), leading to legal liability. A concept developed through Anglo-American case law, tort is the assumption that citizens owe each other a duty of care. If the third party suffered a loss due to an individual's actions, he or she could sue that person for compensation.

[221] Person who brings a case against another in a court of law.

[222] The individual, company or institution sued or accused in a court of law.

[223] Prosser, W. Privacy. *California Law Review*, 1960, 48, 383-423.

[224] Linowes, D.F. and Bennett, C. Privacy: its role in federal government information policy. *Library Trends*, 1986, 35 (1) 22.

[225] The outer regions of other specified rights such as freedom of speech (first amendment) and protection against unreasonable search and seizure (fourth amendment). Related to this concept is the ninth amendment – which declared that just because certain rights are not mentioned in the Constitution does not mean they do not exist.

[226] Linowes, D.F. and Bennett, C., ref. 224, p. 22.

[227] Miller, A. *The assault on privacy*, 1971.

[228] Westin, ref. 216.

[229] United States. *Freedom of Information Act*, 5 USC 552, 1966.

[230] *Ibid.*, section 6 (b).

[231] This practice was never tested in court, and stopped after a 'conference committee' from both Houses of Congress made it clear that protection of privacy was not intended to justify such refusal of what is now known as subject access. See Michael, J. ref. 76, p.83.

[232] Westin, A. ref 216., p. 387.

[233] Michael, J. ref. 88, p.84.

[234] United States Supreme Court. *Federal Aviation Administration Robertson v. Robertson*, 422 US 255 (1975). URL: http://laws.findlaw.com/us/422/255.html [Accessed 16/01/03]. Refer:

- Michael, J., ref. 88, p.85.

[235] United States. *Privacy Act*, 5 USC 552a, 1974.
URL: http://www.epic.org/privacy/laws/privacy_act.html [Accessed 16/01/03].

[236] Michael, J., ref. 88, p.83. Watergate is the name given to a major US political scandal. It began with a burglary and wiretapping of the Democrat Party's headquarters and later engulfed President Nixon and many of his supporters in a variety of illegal acts – including creation of false and slanderous documents casting political opponents in a false light. The scandal culminated in Nixon's resignation in August 1974.

[237] This was the major source of controversy as the law was debated. Senator Ervin introduced a Senate bill providing for a Federal Privacy Board with oversight advisory responsibilities. However, Ervin was forced to abandon this notion due to: irreconcilable differences between House and Senate; the desire to produce some legislative response to Watergate; and the fear of a presidential veto if the bill contained a provision for an independent and permanent privacy commission. This climbdown resulted in the establishment instead of the Privacy Protection Study Commission to investigate the issue and make recommendations to the President and Congress for action.

[238] United States. Privacy Protection Study Commission. *Personal Privacy in the Information Society*, 1977. US Government Printing Office, 20402.

[239] *Ibid.*, Chapter 13, Conclusion (1), page 502.

[240] Linowes, D.F. and C. Bennett., ref. 224, p.35.

[241] Rule, J. et al. *The politics of privacy*, 1980, p.103.

[242] These figures are from the US Department of Commerce. For more detailed figures relating to US-EU trade refer to Delegation of the European Commission to the United States, URL: http://www.eurunion.org/profile/EUUSStats.htm [Accessed 16/01/03].

[243] The FAQs supplement the principles – providing guidance to certain sectors of industry and branches within US organisations. Provision include: sensitive data (FAQ 1); investment banking and audits (FAQ 4); human resource data (FAQ 9); and airline passenger reservations (FAQ 13).

The principles are detailed on the US Department of Commerce's 'Safe Harbor' website, URL: http://www.export.gov/safeharbor/sh_documents.html [Accessed 16/01/03].

[244] *Directive 95/46/EC*, ref.45., Article 26 (1) (b) and (c).

[245] *Ibid.*, Article 26 (2).

[246] European Communities. Commission. *Data protection: standard contractual clauses to facilitate personal data transfers to third countries for processing*. Brussels, 22/01/02. URL: http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/02-102.htm [Accessed 16/01/03].

[247] European Communities. Commission. *Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce.* Official Journal of the European Communities. No. L215/7. (25.8.2000).
URL: http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/index.htm [Accessed 16/01/03].

[248] The letters between the DOC and the European Commission during March 2000 and June 2000 are documented on the Department of Commerce's 'Safe Harbor' website, ref. 243.

[249] On 5 July 2000, the European Parliament passed a Resolution by 279-259 criticising the 'Safe Harbor' principles for providing insufficient remedies to individuals, and calling on the European Commission to reopen negotiations. The Internal Market Commissioner, Frits Bolkestein, overruled Parliament on 13 July 2000 – proposing the Commission adopt the 'Safe Harbor' principles. This was duly achieved on 26 July 2000.

[250] FAQ 9 Human Resources, ref. 243.

[251] United States. *Federal Trade Commission Act.* 15 USC 41-51, 1914.

[252] Refer to overview on Safe Harbor website: URL: http://www.export.gov/safeharbor [Accessed 16/01/03].

[253] *Ibid.*

[254] European Communities. Commission. *The application of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce.* Brussels, 13/02/02. SEC (2002) 196. URL: http://europa.eu.int/comm/internal_market/en/dataprot/news/index.htm [Accessed 16/01/03].

[255] Jonquieres, G. de. EU "no" to data privacy delay. *FT.com*, 06/05/01. URL: http://www.ft.com [Accessed 16/01/03].

[256] Arthur, C. Now Bush wants to scrap deal on internet privacy. *The Independent*, 31/03/01. URL: http://www.independent.co.uk [Accessed 16/01/03].

[257] Meller, P. EU expected to reject longer data retention. *ITworld.com,* 12/11/01. URL: http://www.itworld.com/Man/2681/IDG011112EUdataprotection/ [Accessed 16/01/03].

[258] Rosenbaum, A. and R. MacMillan, EC data protection amendment could help heal rift with US. *Newsbytes*, 31/01/02. URL: http://newsbytes.com/news/02/174125.html [Accessed 16/01/03].

[259] Weardon, G. US tech protests EU privacy laws. *ZDNet*, 30/09/02. URL: http://zdnet.com.com/2100-1106-960134.html [Accessed 16/01/03].

[260] Canada. Department of Communications and Department of Justice. *Privacy and Computers: a report of a Task Force.* Ottawa, 1972.

[261] For detailed analysis of early Canadian attempts at privacy legislation, refer to:

- Flaherty, D., ref. 92, pp.243-301.

[262] New Scientist. 'The public is sick to death'. *New Scientist*, 13/10/77, p.92.

[263] Canada. *Privacy Act*, (R.S. 1985, c. P-21). URL: http://laws.justice.gc.ca/en/P-21/ [Accessed 16/01/03].

[264] Canada. *Personal Information Protection and Electronic Documents Act.* (2000, c.5). URL: http://laws.justice.gc.ca/en/P-8.6/ [Accessed 16/01/03].

[265] Privacy Commissioner of Canada. Frequently Asked Questions. URL: http://www.privcom.gc.ca/faq/faq_01_e.asp#001 [Accessed 16/01/03].

[266] The House of Commons Justice and Solicitor General Committee published over 100 recommendations for improving the provisions of the Privacy Act in 1987. Refer:

- Flaherty, D., ref. 92, pp.297-301.

[267] Canadian Standards Association (CSA). 1996. *Model Code for the Protection of Personal Information*, ref. 39.

[268] Canada. Quebec. *An Act respecting the protection of personal information in the private sector.* (c. P-39.1) Updated to 01/11/02. URL: http://www.canlii.org/qc/sta/csqc/20030131/r.s.q.p-39.1/whole.html [Accessed 23/05/03].

[269] Privacy Commissioner of Canada. Privacy legislation in Canada. URL: http://www.privcom.gc.ca/fs-fi/fs2001-02_e.asp [Accessed 07/05/03].

[270] Canada. *Personal Information Protection and Electronic Documents Act*, ref. 264. Schedule 1, clause 4.3.6.

[271] *Ibid.*, Schedule 1, clause 4.7.2.

[272] Part of this responsibility includes submitting an annual report to Parliament. This can cause controversy. The 1999-2000 report revealed the existence of a government database called the Longitudinal Labour Force File which contained over 2000 pieces of information on each Canadian. The information was gleaned from other government data banks and included details from tax returns, child tax benefit files, welfare files, federal jobs, employment insurance files and the social insurance master file. In May 2000, the government announced that the file was being dismantled following a public outcry, and that the software which allowed sharing with other agencies was being scrapped.

[273] *Commission Decision 2002/2/EC*, ref. 211.

[274] Canada. *Anti-Terrorism Act*. (2001, c.41). URL: http://canada.justice.gc.ca/en/terrorism/ [Accessed 16/01/03]. This came into law on 24/12/01.

[275] Canada. *Aeronautics Act*. (1977, c.A-2), section 4.83. URL: http://laws.justice.gc.ca/en/a-2/290.html [Accessed 16/01/03].

[276] Bennett, C.J. Privacy protection in Canada and the US: the implications of September 11th. *Privacy Conference*. Rathenau Institute, The Hague, Netherlands, 17/01/02.

[277] *Ibid.*

[278] Bennett, C.J., ref. 1.

[279] Bennett, C.J., ref. 276.

# Fully compliant? A study of data protection policy in UK public organisations

## Volume 2

by

**Adam Warren**

A Doctoral Thesis

submitted in partial fulfilment
of the requirements for the award of the degree of
Doctor of Philosophy
of
Loughborough University

June 2003

Department of Information Science

# Fully compliant? A study of data protection policy in UK public organisations

## Volume 2

## Contents


**5. Safeguarding data protection: the wider legal context** 191

**5.1 Introduction** 191

5.1.1 Objectives

**5.2 European Convention on Human Rights** 193

5.2.1 Key terms and concepts

5.2.2 Article 8: right to privacy

*Limits on Article 8*

5.2.3 Interface with freedom of expression

5.2.4 Strasbourg case law

**5.3 UK Human Rights Act 1998** 200

5.3.1 Provisions

5.3.2 Incorporation of ECHR into UK law

5.3.3 UK human rights case law

5.3.4 Official guidance

5.3.5 Issues for public organisations

**5.4 Freedom of Information Act 2000** 209

5.4.1 Context: FOI overseas

5.4.2 Context: FOI in the UK

5.4.3 FOIA 2000: access to information?

*Provisions*

*Delays in implementation*

*FOIA Scotland*

5.4.4 FOI and data protection

**5.5 Interception and retention of communications data** 218

5.5.1 RIPA 2000: context

5.5.2 *Lawful Business Practice Regulations*: undermining data protection?

5.5.3 Anti-Terrorism, Crime and Security Act (ATCSA) 2001

*Provisions affecting data protection*

**5.6 Conclusions** 224

**6. Findings: questionnaire survey and expert interviews** **235**

**6.1 Expert interviews** 236

6.1.1 Data Protection Act 1998

6.1.2 Employment practices

*EU working paper and possible moves toward legislation*

*UK code of practice*

*Towards collective agreements?*

6.1.3 Transfer of personal data to third countries

6.1.4 Policy: data protection in organisations

*E-government*

*Safeguarding personal data online*

6.1.5 Human Rights Act 1998

6.1.6 Freedom of Information Act 2000

6.1.7 Anti-terrorism

6.1.8 Conclusions

**6.2 Questionnaire survey** 258

6.2.1 Data analysis

6.2.2 Conclusions

**7. Findings: case studies** 283

**7.1 Introduction** 283

7.1.1 Nature of organisations studied

7.1.2 Criteria for compliance

**7.2 Status of data protection function** 291

7.2.1 Training

7.2.2 Staffing and resources

7.2.3 Location of data protection function

**7.3 Public awareness** 300

**7.4 Staff awareness and training** 301

7.4.1 Methods

*Staff presentations*

*Intranet and video*

*Induction*

*Training packages*

7.4.2 Targeted training

7.4.3 Difficulties facing local authorities

7.4.4 Towards compliance?

**7.5 Handling subject access requests (SARs)** 310

7.5.1 Procedures

7.5.2 Volume of SARs

7.5.3 Charging for subject access

**7.6 Data protection policy** 317

7.6.1 Influences

7.6.2 Policy development

*Local authorities*

*Universities*

*Other case study organisations*

7.6.3 Data protection 'built-in'?

7.6.4 Evaluation

**7.7 Conclusions** 335

**8. Conclusions and recommendations** **344**

**8.1 Outline of thesis: aim and hypotheses** 344

**8.2 Hypothesis 1: compliance and good practice** 346

*Analysis of objectives*

**8.3 Hypothesis 2: privacy and the interface with other key legislation** 347

*Analysis of objectives*

**8.4 Recommendations** 351

8.4.1 Stakeholders

8.4.2 Further research

**Bibliography** **364**

## Figures

2. Measures taken to comply with the Data Protection Act 1998 261

3. Provisions for employees requesting their own personal data 263

4. Procedures for safeguarding security of employee records 264

5. Frequency of monitoring of staff email and internet usage 267
6. Respondents monitoring staff email and internet usage automatically 268
7. Respondent awareness of legislation and official guidance 269
8. Respondent views on the *Lawful Business Practice Regulations* and the Data Protection Act 1998 270
9. Respondent views concerning the impact of the Human Rights Act 1998 271
10. Respondent views concerning official guidance on the Data Protection Act 1998 and the Human Rights Act 1998 272

**Tables**

6. Questionnaires received by category 259
7. Respondents with nominated staff responsible for data protection 260
8. Policy concerning staff email and internet usage 265
9. Respondents monitoring staff email and internet usage 266

**Appendices** **I**

**Appendix A:** Interview: Sir Norman Lindop – 6 September 2001 I
**Appendix B:** Copy of Home Office letter dated 15 November 2001 re Lindop papers VI
**Appendix C:** Pilot questionnaire - *Privacy and human rights in the workplace* VIII
**Appendix D:** Full questionnaire - *Privacy and human rights in the workplace* XIII

# 5. Safeguarding data protection: the wider legal context

## 5.1 Introduction

Since the enactment of the DPA 1998, a number of statutes have been passed in the UK impacting on eight principles that form the backbone of the legislation. This Chapter analyses the subsidiary hypothesis 2, assessing how effectively the DPA 1998 works with other legislation impacting on data protection. Perhaps the most far-reaching statute has been the Human Rights Act (HRA) 1998, incorporating the provisions of the European Convention on Human Rights (ECHR) into UK law. A key part of the ECHR is Article 8 - right to a private life. Sections 5.2 and 5.3 will address the context to, and provisions of, the HRA 1998 – whether it introduces a right to privacy into UK law, and if so, whether it represents a clear and workable provision. Section 5.2 examines the ECHR - its hierarchy of rights, and the principles of interpretation to be followed by the UK courts when examining human rights issues. From the outset, reference has been made to Article 8 and how it may interface with Article 10 – freedom of expression. Case law from Strasbourg has been assessed to determine any precedents that may be followed by UK courts.

Section 5.3 focuses specifically on the HRA 1998. The key provisions of the Act are outlined, and commentary from academics and leading lawyers examined to assess how the HRA 1998 will work out in practice. The small amount of case law in existence has been analysed for any precedents or patterns, and attention given to any difficulties in incorporating legislation from a different legal culture into UK law. As the HRA 1998 explicitly applies to 'public authorities', this section will examine how aware such organisations are of the legislation, the official guidance received and whether current practices need to be radically altered in order to safeguard the right to privacy.

Section 5.4 considers the challenges posed by the new Freedom of Information Act (FOIA) 2000, which will be fully implemented by 2005. Unlike the DPA 1998, FOIA 2000 was not enacted to implement an EU directive in the field.

Rather, it was passed by the UK Labour government following promises made in its 1997 election manifesto. The context to, and the provisions of, FOIA 2000 are investigated. Issues addressed include: the status of FOIA 2000 in UK law; the mechanisms established to regulate the Act; and the interface of FOIA 2000 with the DPA 1998. This statute deserves consideration for two key reasons. Firstly, it specifically alters and extends the scope of the DPA 1998 to include manually personal data that is held in an *unstructured* format. The implications of this change are discussed in subsection 5.4.4. Secondly, FOIA 2000 – in providing for access to information generally – complements the DPA 1998, with its emphasis on protection of personal information. Indeed, when requesting personal data concerning third parties one Act cannot be considered without the other. The demands of both laws have prompted organisations to review their policy-making in relation to handling of personal data, with both data protection and freedom of information being considered in tandem. The consequences for the way organisations handle information privacy are introduced in this Chapter, and elaborated in the fieldwork analysis in Chapters 6 and 7.

Section 5.5 considers the final two laws discussed in this Chapter: the Regulation of Investigatory Powers Act (RIPA) 2000 and the Anti-Terrorism, Crime and Security Act (ATCSA) 2001. Both Acts were passed in response to international concerns. RIPA 2000 enacted part of the EU's Telecommunications Data Protection Directive 97/46/EC, whilst the ATCSA 2001 was passed in reaction to terrorist attacks in the US. Both have implications for data protection, in particular regarding: interception of communications data; retention of personal data by data controllers; and access to personal data by law enforcement agencies. Section 5.5 will assess the extent to which the UK government has built human rights and data protection safeguards into these statutes.

Finally, this Chapter concludes with implications of these measures for public organisations attempting compliance with the DPA 1998. This Chapter thus provides a foundation for the fieldwork analysis undertaken in Chapters 6 and 7.

### 5.1.1 Objectives

The objectives of this chapter are to:

- Identify the main provisions of the recent key UK legislation affecting the provisions of the DPA 1998. The legislation referred to are: HRA 1998; FOIA 2000; RIPA 2000; and ATCSA 2001;
- To set the above statutes in context, and assess their impact on public organisations attempting compliance with the DPA 1998.

## 5.2 European Convention on Human Rights

In 1948, the United Nations General Assembly adopted the Universal Declaration of Human Rights, with thirty Articles covering a full range of civil, political, economic, social and cultural rights in one document. Article 12 stated:

> 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.'[1]

Member countries were called on to publicise the text of the Declaration 'principally in schools and other educational institutions'[2]. The adoption of the European Convention on Human Rights (ECHR) in 1950 gave specific legal content to the rights contained in the Declaration.

### 5.2.1 Key terms and concepts

The ECHR is fundamental, being at the top of the European legislative tree. Both Convention 108[3] and the 1995 Data Protection Directive[4] made explicit reference to the ECHR, including respect for the private domain. As the Data Protection Act 1998 was enacted to implement the Directive, it thus had its roots firmly in the ECHR. The Convention guaranteed numerous rights and freedoms[5] including:

- The right to life (Article 2);
- Prohibition of torture and inhuman or degrading treatment and punishment (Article 3);
- Prohibition of slavery and forced labour (Article 4);
- The right to liberty and security (Article 5);
- The right to a fair and public trial (Article 6);
- The right to respect for private and family life, home and correspondence (Article 8);
- The right to freedom of expression (Article 10).

This section will be concerned with the latter two Articles. There is a hierarchy of Convention rights: some are absolute, some can be limited, and others are qualified. Absolute rights cannot be derogated from and include protection from torture and prohibition of slavery. Other rights, such as the right to a fair trial can be limited under explicit and finite circumstances defined in the ECHR itself. Finally, qualified rights include the right to a private life and the right to freedom of expression. Interference with these rights is permissible subject to various qualifications – for example, that any restriction must have its basis in law, be necessary in a democratic society and be related to the permissible aim set out in the relevant Article (for example, the prevention of crime).

Adopted by the Council of Europe in 1950 to prevent totalitarianism and a repeat of the atrocities of the Second World War, the ECHR sought to protect fundamental rights and freedoms against the power of the state. This meant that the rights could be relied on by any victim who claimed that his or her civil liberties had been or would be interfered with. This could be an individual, non-governmental organisation or group of individuals and in some cases also companies and other bodies[6]. However, these rights did not apply to governmental organisations such as local authorities. The ECHR contained other provisions, largely about the machinery for enforcing rights, which have not been incorporated by the HRA.

The European Court of Human Rights was established in Strasbourg to decide on disputes involving the ECHR. In its judgements, the Court has adopted a number of principles of interpretation of the ECHR:

(i) It is to be given a broad and generous interpretation rather than a strict legalistic interpretation. Its purpose is the protection of human rights and fundamental freedoms, and to maintain and promote the ideals and values of a democratic society;

(ii) It is a 'living instrument' (*Tyrer v UK* 1976 2 EHRR 1)[7] which must be interpreted in the light of present day conditions. Societies and values change, and the Strasbourg court takes account of these changes in interpreting the Convention. In doing so, it looks to see whether there are common European standards;

(iii) In relation to some Convention rights – such as those requiring a balance to be struck between competing considerations – the Strasbourg court allows a 'margin of appreciation' to the state, and is reluctant to substitute its own views of the merits of the case for that of the domestic authorities;

(iv) Terms and expressions in the ECHR have the same meaning for all the countries bound by it. The meaning is given independently by the Strasbourg authorities. The use of an expression in the law of an individual state (such as whether the matter is considered to be criminal or civil) is not conclusive and may not be the same as the definition of that expression in the Convention.

The ECHR provided a mechanism for individuals to enforce their rights against states, allowing a right of 'individual petition', as well as permitting states to bring proceedings against one another. In 1966, the right of individual petition was granted in the UK. This allowed individual litigants in the UK to seek redress in international law where no adequate remedy could be provided by the domestic courts. Since November 1998, all cases have been dealt directly by the European Court of Human Rights in Strasbourg, and its decisions were binding on the country concerned[8]. The process of application is twofold. Firstly, the Court decides if a claim is admissible – that is, it falls within its terms of reference[9].

Secondly, the Court considers the merits of the application – attempting in the first instance a negotiated agreement between the applicant and the government. Failing that, further written and oral submissions are made by both parties before the Court comes to a decision concerning the violation of individual rights.

### 5.2.2 Article 8: right to privacy

Article 8 of the ECHR protected the right to respect for a person's private and family life, home and correspondence. A qualified right, Article 8 is divided into two parts:

> '(1) Everyone has the right to respect for his private and family life, his home and his correspondence.
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'[10]

The majority of case law has been concerned with defining the terms 'private life', 'family life', 'home' and 'correspondence'[11]. Article 8 has been used in a wide range of contexts: from phone tapping to the right to practise one's sexuality. The European Court of Human Rights has held that the essential object of Article 8 is to protect the individual against arbitrary action by the public authorities (*Kroon v Netherlands*, 1994, 19 EHRR 263).

Interference by the state must be justified by one of the exceptions detailed in Article 8 (2), and be the minimum necessary. Only these exceptions, along with the restrictions in Article 17 (prohibition of abuse of rights), are permitted. Once the state has identified an exception, the Court will then focus on proportionality – whether the interference serves a 'pressing social need'[12].

In terms of 'private life' the Court ruled in *Niemetz v Germany* (1992, 16 EHRR 97) that the concept of private life was to develop one's own personality as well as one's right to create relationships with others. It would be too restrictive to limit the notion of privacy to an inner circle where the individual may live his life entirely as he chooses to the total exclusion of the outside world. Thus respect for a private life must comprise, to a certain degree, the right to establish and develop relationships with other human beings. Additionally, 'private life' can be extended to the office context, for example, in *Halford v UK*, (1997, 24 EHRR 523), it was held that the bugging of private telephone calls made from an office telephone could constitute a violation of the right to respect for private life.

In terms of 'family life', the case law has turned on the evolving definition of what is meant by family – now extending beyond formal relationships and legitimate arrangements, for example, to children born outside wedlock. The concept of 'home' has been judged to overlap with private life in certain circumstances. In *Niemetz v Germany*, (1992, 16 EHRR 97) the Court extended the notion of privacy to include some places of work. The case involved a police search of a lawyer's office. The Court held that Article 8 protected the lawyers' office space, as one's private life was carried out both at 'home' and, at times, elsewhere, including the office. This could have implications for employee privacy.

Finally, the right to respect for one's 'correspondence' is a right to uninterrupted and uncensored communication with others. In the *Halford* case, it was found that Article 8 was violated with respect to calls made from the applicant's office because there was no legal regulation of it. This has been remedied by RIPA 2002, in particular, its *Lawful Business Practice Regulations*.

*Limits on Article 8*

Article 8 (2) stated the limitations on the right to a private life. To prevent any interference violating Article 8, it must fulfil two criteria:

(i) It must be 'in accordance with the law' – in the UK that would relate to the common law of confidentiality and the statutory provisions on data protection;

(ii) It must be 'necessary in a democratic society', meaning that any violation of the right to privacy must be no greater than is necessary to achieve the intended objective. For example, if data for research was used in a form whereby individuals could be identified when it could have remained anonymous.

However, the above criteria are so vague, that it can be argued they undermine the right to privacy. For instance, surveillance could be justified under the *Lawful Business Practice Regulations*, discussed in section 5.5.2 of this Chapter.

5.2.3 Interface with freedom of expression

The interplay between Article 8 (privacy and its intentions) and Article 10 (freedom of expression and its limitations) ask some of the most fundamental questions in a democratic society, especially one with a powerful press such as the UK. The European Court of Human Rights has recognised the essential role of the media as a public watchdog and has declared wide support for freedom of expression. However, argued Williams[13], the Court has done little to consider the relationship between privacy and freedom of expression: both are heavily qualified and neither has obvious priority over the other. Nor has Strasbourg arrived at a very settled position regarding the nature of 'political' speech, what is of public interest, or the extent to which false speech is permissible. However, Williams concluded that a hierarchy has been recognised whereby the greatest latitude must be accorded to critics of the government, and the narrowest to those who attack the reputation of private citizens.

In the UK, the government has attempted to reassure the media that privacy claims will not easily trump freedom of expression. Section 12 of the HRA 1998 requires courts to pay 'particular regard' to the importance of the Article 10 when deciding whether to grant any relief in respect of 'journalistic, literary or artistic merit'[14]. It

remains to be seen whether this will significantly alter existing practices in UK courts.

### 5.2.4 Strasbourg case law

According to Jay's assessment of Strasbourg case law[15], the objects and purpose of the Convention were: the protection of individual human rights (*Foering v UK*, 1989, 11 EHRR 439), and the maintenance and promotion of the ideals and values of a democratic society. These supposed 'pluralism, tolerance and broadmindedness' (*Handyside v United Kingdom*, 1976, 1 EHRR 737), the rule of law and the preservation of freedom of expression.

Recent cases have reinforced the individual's right to protection of personal data as part of the fundamental rights and freedoms guaranteed by the Convention. *Amman v Switzerland* (2000, 30 EHRR 843) involved the recording of a telephone conversation between a Swiss businessman and a client, coupled with the creation and storing of personal data concerning the applicant on a card index. Both practices, committed by the Public Prosecutor, were deemed to violate the ECHR as they had no legal basis in Swiss law. Moreover, in spite of a provision in the national data protection law providing that data which turned out not to be 'necessary' should be destroyed, this did not occur once it emerged that no prosecution was being prepared. A further case, *Rotaru v Romania* (2000)[16] concerned the storing and use of personal data about a retired lawyer by the Romanian Intelligence Service. The data contained information – some of which had been declared false – about the applicant's studies, political opinions and criminal record. This data was found to be held and processed not 'in accordance with the law'. Moreover, the applicant had been refused the opportunity to refute its accuracy. Therefore, a violation of Article 8 had occurred. In deciding both judgements, Strasbourg not only drew on previous case law such as *Halford* and *Niemetz*, but also Convention 108 in safeguarding the individual's 'right to privacy with regard to the automated processing of personal data relating to him'[17].

## 5.3 UK Human Rights Act

### 5.3.1 Provisions

The HRA 1998 obtained Royal Assent on 9 November 1998, but its commencement was delayed under 2 October 2000 to allow time for an extensive programme of judicial education to take place. The Act radically altered the interpretation and use of other UK legislation. The overall objective was to incorporate the Convention into the existing legal system, so that all courts will consider ECHR arguments, and rights previously only obtained in Strasbourg could be secured in national courts. Some of the key provisions are outlined below.

Section 1 and schedule 1 of the Act defined the Convention rights that had been incorporated. Section 2 required that any court or tribunal determining a question raised in connection with a Convention right took into account Strasbourg case law. Section 3 required primary and subordinate legislation – so far as possible – be read and given effect in a way that is compatible with the ECHR. Importantly, this applied whether the legislation was enacted *before* or after the HRA 1998. Should a declaration of incompatibility is made by the courts, section 10 provided a 'fast-track' procedure whereby the government can amend legislation in order to remove incompatibility with the Convention. Section 6 generally made it unlawful for a public authority to act in a manner incompatible with a Convention right.

Section 7 dealt with proceedings that may be brought by a 'victim'. Section 7 (1)(a) permitted a victim of an act by a public authority that infringed a Convention right to bring proceedings 'in the appropriate court or tribunal'. Section 7 (1)(b) permitted a person to rely on the Convention right or rights concerned in any legal proceedings against the public authority. Section 8 concerned judicial remedies, allowing damages to be awarded if necessary to afford 'just satisfaction'. In determining whether to award damages and the amount to award, the court had to take into account the principles applied by the European Court of Human Rights. Section 11, for avoidance of doubt, provided

that reliance on Convention rights should not restrict reliance on other legal rights, or procedural methods of enforcing them. Finally, sections 12 and 13 provided specific assurances as to the respect which will be afforded to freedom of expression and freedom of thought, conscience and religion. Accordingly, these are 'comfort clauses' for sections of the press and certain religious organisations[18].

### 5.3.2 Incorporation of ECHR into UK law

The ECHR and UK law differ substantially – respectively representing civil and case law. Put simply, the Convention dealt with rights that are fundamental and overarching, not tied to strict and exact language, nor to the doctrine of precedents. In UK law, the language is more detailed and precise, and the doctrine of precedence is applied. According to Jay, the solution adopted by the HRA 1998 combines creativity and pragmatism – leaving, on the face of it, the aforementioned features of the UK legal system untouched: 'the ECHR is not incorporated into UK law so much as infiltrated into it.'[19] The ECHR has been brought into effect by three main means:

(i) The doctrine of interpretation by the UK courts and tribunals (section 2);

(ii) The requirement that statutes and statutory instruments be interpreted in accordance to Convention rights (section 3);

(iii) The requirement that public authorities act in a way compatible with Convention rights (section 6).

As a leading human rights lawyer Lord Lester viewed it, the HRA is a 'code of ethics to steer judges or decision makers generally when they have to make decisions that impact on the rights of individuals.' [20]

Strictly speaking the Act did not incorporate Convention rights into domestic law, but gave 'further effect'[21] to ECHR rights by requiring the courts (section 3 (1)) so far as possible to construe primary and secondary legislation in a way compatible

with Convention rights. To quote the Lord Chancellor, Lord Irvine, when the Human Rights Bill was being debated in the House of Lords:

> "The Bill gives the European Convention on Human Rights a special relationship which will mean that the courts will give effect to interpretative provisions [...], but it does not make the Convention directly justiciable as it would be if it were expressly made part of our law. I want there to be no ambiguity about that..."[22]

Thus the DPA 1998 will now be interpreted in accordance with Convention rights. The Convention rights have been developed over the years by protocols adding property rights, education rights and rights to free elections. However, the Convention will not be directly 'justiciable' – that is, subject to trial in a court of law.

Incorporation of the ECHR has been presented by commentators such as Singh[23] and Palmer[24] as a covert privacy law – potentially filling in the gaps in current UK case law provision. Technically, the legislation only applied to 'public authorities', but the inclusion of courts under this definition (section 6) has led commentators to speculate that a 'horizontal' application of rights (against private industries as well as public authorities) is inevitable[25]. This may mean far more pervasive effect in UK law than might have done had the ECHR been incorporated as overriding law, because the method chosen has increased the likelihood of a powerful horizontal effect of the Convention rights. Certainly, the application of the human rights context reinforces the growing willingness of regulators and courts to look at the purposes of the law and its background in the international instruments which outline privacy rights[26].

### 5.3.3 UK human rights case law

Although the HRA 1998 was only enacted in October 2000, there has been some indication, in the cases judged to date, of the interpretations the UK courts are taking regarding the development English privacy law. As discussed in Chapter 4

(section 4.5.1), privacy protection in English law had been segmented under headings such as trespass, nuisance, defamation and breach of confidence[27]. In Strasbourg, the right to privacy had been developed evenly under the aegis of Article 8. Given the differences in legal culture, it was difficult to envisage how receptive the English judiciary would be to the idea of simple acceptance of the Strasbourg case law evolution under Article 8.

Kearns[28] – an academic lawyer - suggested in March 2001 that on the basis of limited evidence to date, English judges are preferring 'to embrace the European law under Article 8 within the already-established most relevant sector of existing disparate English law on privacy'[29]. Thus European law has been divided in an alien way into separate English doctrines such as trespass and breach of confidence. Kearns backed up this assertion by reference to two major cases. The first – *Douglas and Others v Hello! Ltd* – was discussed in Chapter 3[30]. In this case, the decision published by the Court of Appeal on 16 January 2001 recognised that a breach of privacy had taken place within the bounds of the English doctrine of breach of confidence. However, one of the judges – Lord Justice Sedley – stated that English law could now recognise privacy as a legal principle in its own right, drawn from the fundamental value of personal autonomy. The second case cited by Kearns – *Venables and Another v News Group Newspapers and Others* – was also published by the Court of Appeal on 16 January 2001. It stated only that the court had jurisdiction to extend the protection of confidentiality in exceptional circumstances, such as where not to do so would be likely to lead to serious physical injury or death of the person seeking that confidentiality. Fundamentally, Kearns believed that there was a danger that breach of confidence was being used to accommodate all or the majority of privacy issues, 'implausible though that may seem'[31]. This view has been endorsed by Singh and Strachan, whose review of the development of English privacy law included decisions up to March 2002. Their article was discussed in Chapter 3. Both papers argued that this conservative interpretation of privacy rights by the English judiciary would fail to do justice to the privacy characteristics – private life, family life, home and correspondence – that have evolved under Strasbourg case law, and which should take a similar course under English law.

Recent cases involving data protection include *Regina (Robertson) v Wakefield Metropolitan District Council and Another* and *Campbell v Mirror Group Newspapers.* In the former case, the High Court ruled in November 2001 that individuals had the right to prevent their information held on the electoral register from being used for commercial purposes. In fact, this right had been stipulated in section 9 of the Representation of the People Act 2000 entitled 'Restriction on the supply of information contained in the register'[32]. This allowed regulations to be made resulting in two versions of the electoral register – a complete one and an edited version omitting the names of those who have asked to be excluded from it. Whilst much of the Representation of the People Act came into effect in February 2000, the section 9 provisions were made subject of a consultation. This consultation was completed in June 2001, and a month later the Minister for Local Government and the Regions stated that the government intended to consult further on the section 9 provisions:

> "...with a view to making regulations in the autumn which will provide for a full and edited electoral register with the effect from the 2002 canvas."[33]

In the meantime, an elector in Pontefract, Brian Robertson, requested his local authority to cease making his data available to third parties such as credit reference agencies and direct marketing companies. When Wakefield Metropolitan District Council turned down the request, the applicant refused to make his data available and consequently lost his right to vote in the 2001 general election. On 16 November 2001, the High Court stipulated that the transfer of electoral roll information to third parties without an opportunity to object breached both the DPA 1998 and the claimant's Article 8 right to privacy. Moreover, it amounted to an unjustified restriction on his right to vote, thereby violating the HRA 1998[34]. For a period, many case study organisations suspended the sale of their electoral roll personal data whilst they awaited a response from central government. Following this judgement, the section 9 regulations were finalised[35], taking into account the Court judgement in relation to the requirements of the ECHR, HRA 1998 and the DPA 1998.

The new regulations came into effect on 16 October 2002, establishing the dual register – a full version, with restricted uses[36], and an edited version, sold for any purpose, from which voters can opt out. However, the original complainant is still unhappy. In autumn 2002, Robertson stated that, as the full electoral rolls can still be made available to credit-referencing agencies, he will be refusing once again to complete his form[37]. At the time of writing, Robertson was waiting for a date to argue his case in the High Court.

The case involving Naomi Campbell has been discussed to some extent in Chapter 3. Like Douglas, the court ruled that even celebrities were 'entitled to some space of privacy'[38]. However, this case was more significant in terms of data protection, being the first time a trial court has awarded compensation for breach of the DPA 1998. On 27 March 2002, Mr Justice Morland found that the personal data contained in the material published by the *Mirror* had been obtained unfairly and breached data protection Principle One. Moreover, the judge ruled that publication of the text and photographs of Campbell leaving a meeting of Narcotics Anonymous amounted to processing of sensitive personal data. However, this verdict was overruled by the Court of Appeal on 14 October 2002 when the judges found that the processing of sensitive personal data in the absence of 'explicit consent' was justifiable by journalists as a result of the 'media exemption' in section 32 of the DPA 1998[39]. The clarification of the applicability of this exemption was particularly welcomed by the media, allaying the concerns following the earlier High Court decision. Finally, the Court of Appeal ruled that, as Campbell had previously maintained in the press that she did not take drugs, celebrities could not use the provisions of the DPA 1998 to prevent the media from 'putting the record straight.' In November 2002, Campbell announced her intention to appeal to the House of Lords.

The case law discussed in this sub-section demonstrates the difficulties experienced by UK judges in attempting to balance various ECHR rights – in particular privacy, (Article 8) and freedom of expression (Article 10). Whilst Sedley acknowledged the principle of a distinct right to privacy for all individuals, the courts have been reluctant to express that right in an explicit way. Indeed, UK

courts have tended to rely on extending the tort of breach of confidence, or even using the DPA 1998, rather than developing a clear right to privacy in English law.

### 5.3.4 Official guidance

The UK government has taken some steps to promote compliance with the HRA 1998. Firstly, the Human Rights Unit was set up by the Home Office to maintain and develop the UK's position relating to human rights issues, as well as implementing the HRA. The Unit – moved to the Lord Chancellor's Department in 2001 - has issued a series of guidance documents to the public sector. The document *Core guidance for public authorities: a new era of rights and responsibilities*[40] gave a general outline of ECHR rights and key concepts, along with a checklist for public authorities to determine potential incompatibilities with new legislation. More instructional was *The Human Rights Act 1998: Guidance for Departments*[41], equipped with an action plan which all government departments were instructed to implement. This included a review of current practices and procedures to identify incompatibility with Convention rights, and identified public authorities whose work was linked to relevant department to draw their attention to HRA and ECHR. In October 2002, the above guidance was updated with the publication of a new *Study Guide*[42] and a programme of seminars for those working in public authorities[43].

Pleming[44] examined the measures taken to prepare for the HRA by central government, the police and non-government bodies. He found that whilst the Home Office Human Rights Unit and the Human Rights Task force have done much to ensure compliance with the Act, the absence of a Human Rights Commission – to promote compliance and awareness of the HRA 1998 - has resulted in a relative lack of coordination. More work was required to ensure that public and hybrid authorities are ready for the HRA. Instead of placing the main burden on central government departments, Pleming advocated that the Human Rights Commission should be set up as soon as possible in order to coordinate the review process and become a central specialist advisory body. The desirability of

such a Commission is currently being investigated by the Houses of Parliament Joint Committee on Human Rights[45].

When responsible for human rights, the Home Office set out the main tasks for central government as:

(i) Review of primary and secondary legislation for compliance with Convention rights;
(ii) An assessment of new legislative proposals for compliance with Convention rights;
(iii) Devising a detailed action plan setting out proposals for implementation;
(iv) Staff training to provide a level of awareness of Convention rights;
(v) Ensuring public authorities aware of what they need to do to prepare for implementation.

Indeed, police have conducted their own detailed and sophisticated audit – reviewing existing practices, policies and procedures to identify breaches and potential breaches of Convention rights. This process, which began in November 1998, (earlier than most government departments) filtered out areas in risk groups with those listed as 'critical' undergoing further, in-depth audits. It is intended that such human rights auditing will become part of the culture in the police force, with no new policy or procedure being implemented until it has gone through the screening process.

However, a bulletin from District Audit (2002) reported that – 20 months after the HRA 1998 had come into effect - many local and health authorities were not responding appropriately to the Act[46]. Summarising the findings of a survey of 88 local authorities and National Health Service (NHS) trusts, the bulletin outlined various criteria for ensuring compliance with the HRA 1998 including:

(i) Levels of staff awareness;
(ii) Evidence of a corporate approach;
(iii) Monitoring of compliance with the Act;

(iv) Arrangements ensuring partners, subsidiaries and contractors all take reasonable steps to comply with the Act.

Overall, the survey found that 45 out of 88 local authorities and health bodies had not reviewed their policies and procedures for compliance. Many were adopting a 'wait and see' approach – looking to siphon good practice from other, more active bodies. Health bodies were generally less prepared than local government, leaving themselves vulnerable to legal challenges. The bulletin included examples of good practice, concluding with a checklist for reviewing organisational compliance with the HRA 1998. The provision of half-day seminars across England and Wales, explaining how public services can conform with the provisions of the HRA 1998, was in part a consequence of this bulletin.

5.3.5 Issues for organisations

Wadham and Mountfield have identified several issues for the future[47]. Some of the challenges listed are: new police listening devices; telephone taps; electronic monitoring of worker's use of keyboards; CCTV surveillance; and privacy of employees, particularly in public authorities that will be covered by the HRA 1998. These issues, some of which have been brought before Strasbourg, will be of interest to UK lawyers. To date, the *Robertson* case has had a significant impact on the way public authorities compile electoral rolls. Cases will be brought to test some of the recent regulations and codes of practice in UK. They will be crucial in deciding whether the HRA 1998 does in fact introduce a right to privacy into UK law, and whether it is workable.

Burnes considered the significance of section 7 (1)(b) of the HRA 1998 for employers[48]. As stated in subsection 5.3.1 above, this particular part of the Act allowed a person to rely on Convention rights in any legal proceeding. This might arise where a person wished to use the Act as part of his defence in an action brought by another person. An example of this circumstance would be if an employer intercepted emails or phone calls of an employee, and as a result the employee is dismissed. The employee then appeals against the sacking. In such a

situation, the employee could complain that the interception was unlawful and contravened his rights under the HRA 1998. With the tribunal being a public authority under the HRA 1998, it would not be able to act in a way incompatible with the Act. The employee could make reference to section 7 (1)(b) and Article 8 to argue that a phone call or email had been intercepted unlawfully, therefore the tribunal should exclude the evidence. This may have been precluded by the *Lawful Business Practice Regulations* (refer to 5.5.2 below). Yet, if it has not, the essential point is that whilst the employee could not sue the employer for breach of privacy, they could block the introduction of evidence, and therefore block dismissal. A case heard by an industrial tribunal in November 2000 concerning the dismissal of employees over 'inappropriate' emails actually rejected this argument[49]. However, it is uncertain, argued Burnes, how the courts would react.

## 5.4 Freedom of Information

### 5.4.1 Context: FOI overseas

Freedom of information legislation is intended to give the public greater access to information about the workings of government, thereby improving the democratic process. The Swedish Freedom of the Press Act (1776) is the oldest access law in the world. This Act – now part of the Swedish constitution - required that official documents should 'upon request immediately be made available to anyone making a request' at no charge[50]. The most recent version of that Act was adopted in 1949, and amended in 1976. The rest of the world started to consider FOI legislation as a priority after the Second World War. Reasons for legislating for greater openness of official information included the rise of more pluralistic societies, increasing individualism and a series of political crisis[51]. The US was the first common law state to pass freedom of information legislation, in 1966. This law has been discussed to some extent in Chapter 4 (section 4.7.1). Other freedom of information laws include those of France (1978), Australia (1982), Canada (1983) and Ireland (1997). Most national laws have been updated in recent years to generally increase levels of access, and to take into account electronic records and information.

Within the EU, progress has been slow. During the drafting of the Data Protection Directive 1995, freedom of information issues were in the background. According to an official at Internal Market Directorate General of the European Commission this important question was only discussed at the very end of negotiations[52]. That was encouraged by the accession to the European Community of Sweden in particular, with its tradition of freedom of information[53]. The outcome was Recital 72 of the Data Protection Directive: 'this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive'[54].

During the last decade, the EU has taken steps to provide a greater degree of public access to documents held by Union bodies. Declaration 17 of the Maastricht Treaty 1992 highlighted the need for greater transparency of decision-making[55]. In the Amsterdam Treaty 1997, the EU included a provision in Article 255 allowing 'a right of access to European Parliament, Council and Commission documents'[56]. This provision was implemented by the European Commission through Regulation 1049/2001, which came into force in December 2001[57]. The Regulation permitted access to paper and electronic documents relating to policies, activities and decisions falling within the remit of the EU institutions. A number of exemptions existed, for example, concerning the protection of the public interest and commercial interests, although there were no blanket exclusions from the right to access. A 15 working day time limit for replies was set, and a register of documents held was drawn up during the first half of 2002 to aid public identification of documents.

### 5.4.2 Context: FOI in the UK

In the UK, there was limited activity in the twenty years prior to the enactment of FOIA 2000. In 1979, the Labour government suggest an open government code of practice[58]. In the same year a general election returned the Conservative Party to power. The new government chose not to proceed with the code of practice, and the following decade was marked by the passing of piecemeal FOI legislation such

as the 1985 Local Government (Access to Information) Act 1985[59] and Access to Medical Reports Act 1988[60]. In 1993, the Conservative government moved a step closer to FOI by introducing an *Open Government* White Paper[61]. It recommended a voluntary Code of Practice to be supervised by the Parliamentary Ombudsman. The Code came into effect in 1994. As a non-legal instrument, it did not provide a statutory right of public access to official information through the courts.

The Code was revised in 1997, and again in 1998. Its key features were[62]:

- Official information was released where in the public interest, and in response to 'reasonable' requests;
- Code overseen by the Parliamentary Ombudsman. Whilst the Ombudsman could recommend the release of information, government departments could refuse such requests[63];
- Exemptions from disclosure applied to fifteen categories of information, including:
    - Defence, security and international relations;
    - Communications with the royal household;
    - Law enforcement and legal proceedings;
    - Voluminous or vexatious requests;
    - Privacy of an individual;
    - Statutory and other restrictions.

Nevertheless, the Code did have some positive effects in reducing secrecy. The amount of information routinely disclosed did increase – generally in the form of providing facts and analysis with explanatory material on departments dealings with the public. However, this so-called 'pro-active publishing' was only a small part of the commitment to FOI. Right of access was the key principle, and the exemptions to the Code meant that the balance was with government departments to withhold information. When the Select Committee on the Parliamentary Commissioner held an inquiry into open government in 1996, the Code was considered inadequate. The Committee advocated a FOI Act for the UK[64].

## 5.4.3 FOIA 2000: access to information?

In 1997, a new Labour government came to office, having promised a Freedom of Information Act. A White Paper[65] was published later that year, proposing a liberal enactment – offering an enforceable right to a wide range of public information and restricting access in only a limited number of cases. However, the draft Bill that emerged 18 months later disappointed those campaigning for greater access to government records[66]. It contained an expanded list of exemptions to the right of access and weaker enforcement powers for the independent Information Commissioner – also the supervisory authority for the DPA 1998.

Nevertheless, during its turbulent passage through Parliament, the Bill underwent several amendments improving it as a measure for accessing official information[67]. These included: limiting the use of veto to government departments and certain other bodies; ensuring that exemptions do not apply to statistical information about a decision once it has been taken; and dropping the power to create new exemptions by Parliamentary order. The passage of the Bill through the House of Lords was finally secured in November 2000 when the government came to an agreement with Liberal Democrat peers, permitting four further amendments to the proposed legislation. The main change was to the Bill's public interest test, to ensure the government is more even-handed when deciding whether to disclose information[68].

### *Provisions*

The FOIA 2000 received royal assent on 30 November 2000, and is to come into force in phases. The Act provides a right of access to information held by public authorities including Parliament, central government departments, local authorities, health trusts and schools. Under the Act, access to information held by these bodies is to be granted 'without significant formality, without inquiry into the motives of the applicants and at subsidised cost'[69]. There are, however, 23 exemptions. Some are absolute or class exemptions, which include all information falling within a particular class. Such exemptions are[70]:

- Information accessible to the applicant by other means;
- Information supplied to, or relating to, bodies dealing with security matters;
- Court records;
- Parliamentary privilege;
- Prejudice to the effective conduct of public affairs (only applies to information held by the House of Commons or House of Lords);
- Personal information (where the applicant is the subject of the information, as this is dealt with under the DPA 1998);
- Information provided in confidence;
- Prohibitions on disclosure: where a disclosure is prohibited by an enactment or would constitute contempt of court.

Nevertheless, the majority of exemptions are qualified exemptions: they are only effective where the public interest in maintaining the exemption can be demonstrated to outweigh the public interest in disclosure. Qualified exemptions include[71]:

- Information intended for future publication;
- Defence;
- International relations;
- Relations within the UK;
- The economy;
- Investigations and proceedings conducted by public authorities;
- Law enforcement;
- Formulation of government policy;
- Health and safety;
- Environmental information.

Such exemptions are also known as 'prejudice-based' exemptions: they are only effective in preventing disclosure of information if such disclosure was likely to 'prejudice' certain specified interests. For example, section 36 (1 and 2) of FOIA 2000 states that information held by government departments is exempt from disclosure if disclosure 'would, or would be likely to, prejudice...the effective

conduct of public affairs'. The use of the word 'prejudice' (as opposed to 'substantial prejudice') was subject to some criticism during the drafting of this legislation[72]. For further discussion of this point, refer to the subsection on FOIA Scotland – under which partial exemptions are indeed subject to the stricter 'substantial prejudice' test.

On 30 January 2001, a new Office of the Information Commissioner (OIC) was established to enforce rights of access under FOIA. The OIC, formerly the Office of the Data Protection Commissioner, now supervises both the FOI regime established under the Act and the data protection regime under the DPA 1998. In most cases, the Commissioner is entitled to overrule the decisions of public authorities not to disclose information where he believes that those decisions contravene the requirements of the Act. However, this may be subject to an 'Executive override', where the public authorities can obtain a signed certificate from a Cabinet Minister overruling the OIC's decision. There is no right of appeal against the Ministerial certificate, effectively a government veto on the disclosure of information.

The OIC's role in balancing the public interests in disclosure and non-disclosure will be crucial in ensuring that the Act becomes an effective tool for public openness. Concerns were expressed during the Bill's passage through Parliament about the same body being responsible for supervising the enforcement of two Acts with potentially conflicting functions[73]. However, this combined approach has the advantage that there will not be, as in Canada, a conflict between two groups of enforcement authorities. Moreover, there will be a more consistent interpretation of the interface between the laws. Appeals from a decision of the Commissioner can be brought to the Information Tribunal.

Each public authority must adopt a scheme for publication of information. The schemes must be approved by the OIC, and specify the following:

- The classes of information the public authority intends to publish;
- The manner of publication;

- Whether the information will be made available to the public free of charge.

Public authorities have 20 working days in which to respond to access requests. They may charge a fee, which will be calculated according to Fees Regulations[74]. If a fee is required, the 20 working days will be extended by up to three months until the fee is paid.

An offence of tampering with personal data has also been created. Section 77 of FOIA states that an offence is committed if, following an access request, any person 'alters, defaces, blocks, erases, destroys or conceals' any record which the recipient may have been entitled to.

The Act is far from flawless. In particular, the extensive number and scope of the exemptions to the right of access to information have been widely criticised by organisations such as the Campaign for Freedom of Information Nevertheless, FOIA 2000 is like to prove an extremely useful tool for various applicants – individual citizens, investigative journalists, members of interest and pressure groups, commercial organisations and lawyers. The effectiveness of the Act largely depends on the willingness of such applicants to use the mechanisms established under FOIA 2000 to their fullest extent.

*Delays in implementation*

Since enactment of the Act in November 2000, the government's enthusiasm for freedom of information has waned. Under section 87 of the Act, FOIA has to be in force no later than five years after royal assent – that is, by 30 November 2005. The government had originally stated that it planned to phase it in much earlier, starting with bodies that were already subject to the open government Code. Initially, the intention had been to implement rights of access for central government 18 months after royal assent (by summer 2002), with other authorities phased in at intervals thereafter[75]. Each class of public authority would first comply with the Act's duty to produce a publication scheme, and then with right of access. However, this approach was apparently blocked by the Prime Minister,

Tony Blair, who was said to have been alarmed at prominent figures using the DPA 1998 to obtain their own files[76].

The delay in implementation was confirmed by the Lord Chancellor, responsible for FOI since June 2001, in an announcement to the House of Lords in November 2001[77]. He stated that the right of access would come into force for all public authorities at once, in January 2005 – over four years after the Act's passage in November 2000. This is a longer delay than any other country in the world[78], and sends out a poor signal concerning the government's commitment to FOIA which may be reflected in the approach taken by officials to the legislation. The public authority publication schemes are currently being phased in[79].

*FOIA Scotland*

The Scottish Parliament passed a Freedom of Information Act[80] in April 2002. This separate legislation will apply to public authorities dealing within the competence of the Scottish Parliament (for example, Scottish educational establishments). Generally, the freedom of information provisions in Scotland are more far-reaching. Where exemptions are partial, there will be a higher test of 'substantial prejudice' rather than just 'prejudice' as in the UK law. Moreover, unlike the UK, factual information used in policy formation can be released. A separate, independent, Information Commissioner will be appointed by the Scottish Parliament with the power to order public bodies to release documents on request. This has been necessary as the Information Commissioner in Scotland will be enforcing a different piece of legislation, with different standards, to that applied in the UK.

However, campaigners perceive that the UK Commissioner may take a more liberal interpretation to the exemption test given in FOIA 2000 as a result of the legislation in Scotland: "It can't be in the public interest to keep it secret in the UK if it's disclosed without damage in Scotland."[81] No timetable for implementing the Act has been announced, however it must be fully in force by 31 December 2005[82].

5.4.4 FOI and data protection

Unlike the DPA 1998, the FOIA 2000 is not part of European legislation. Thus, in theory protection of personal data is given legal precedence over rights of access. The relationship between the two Acts is complex. FOIA 2000 does not deal with individual requests to access their own personal information. Rather, FOIA 2000 sets in place mechanisms to ensure that any such requests continue to be handled in accordance with the DPA 1998. However, where an application for personal information is made by someone other than the data subject (the person to whom the information relates), it is governed by FOIA 2000. Nevertheless, the disclosure of personal information to someone other than the data subject is very likely to infringe the data protection principles. Public authorities receiving such requests will, accordingly, usually be exempt from their duties as a result of an exemption provided in section 40 (2) of FOIA 2000.

FOIA 2000 expands the range of personal data held by a public authority to which an individual can have access to under the DPA 1998. Prior to the Act, the DPA 1998 generally only covered manually processed data in a 'structured' form - that is, in a 'relevant filing system'. For example, a hand-written card index system, ordered by reference to individuals' surnames, would fall within this definition. However, a random file of correspondence received by an organisation within a particular month would not. Following the new Act, this provision has been extended to cover all 'unstructured personal data', including the random file of correspondence. This amendment was necessary to bring the DPA 1998's provisions regarding access to personal information in line with FOIA provisions allowing access to non-personal information, regardless of the way in which it was stored. Moreover, it is symbolic – in principle, extending privacy protection to *all* forms of personal information, no matter how poorly organised.

The implications of this legislation for public authorities, in addition to those brought about by the DPA 1998, are considerable. In the words of one case study interviewee at a university:

> "If you look at FOI and DP, everything that isn't covered by one is covered by the other – they've got the whole public authority records wrapped up between them."

As analysed in Chapter 7, in particular, this has resulted in a more coordinated approach to policy-making concerning information, and often to the creation of a new post – combining responsibility for data protection and freedom of information.

Public authorities are now responsible for adopting and maintaining publication schemes, and releasing information, not covered by an exemption, within 20 working days of the request. Where an authority decides not to release information, because it considers an exemption applies, it must give reasons for its decision and must inform the applicant of their right to complain to the OIC. The full implications of the new Act will be discussed in the analysis of case studies in Chapter 7. Official guidance concerning FOI has been drafted by the Lord Chancellor's Department[83] and the OIC[84].

## 5.5 Interception and retention of communications data

Since the enactment of the DPA 1998, a key test of its effectiveness has been with regard to the interception and retention of communications data. This section considers the Regulation of Investigatory Powers Act (RIPA) 2000 and the Anti-Terrorism, Crime and Security Act (ATCSA) 2001. Both have implications for data privacy – concerning interception of communications, retention of personal data by data controllers and access to personal data by law enforcement agencies.

### 5.5.1 RIPA 2000: context

Article 5 (1) of the Telecommunications Data Protection Directive 97/66/EC (refer to Chapter 4, section 4.3.4) aimed to protect the confidentiality of communications made by means of a public telecommunications network. Under the terms of this Directive – recently revised by the EU – this requirement extended to all types of

electronic communication sent by such a network, including fax and email. The obligation also extended to communications on private networks (for example, office telephone networks or email systems), which will also travel - or have also travelled - on a public network. However, the Directive left scope for member states to authorise the interception of communications by businesses when this is necessary for the purpose of providing evidence of business communications. Although the majority of provisions in the Directive had to implemented by October 1998, an exemption was made for Article 5 for which a deadline of 24 October 2000 was set.

Within the UK, the provisions were implemented as RIPA 2000. RIPA repealed the Interception of Communications Act 1985, providing for a new regime to govern the use of intrusive investigative techniques, including interception. Reflecting changes in the communications industry over the previous 15 years, RIPA 2000:

- Created offences of unlawful interception on public telecommunication systems, and a tort of unlawful interception on a private telecommunication system by the operator of that system;

- Authorised the interception of communications in cases where the interceptor has reasonable grounds to believe that both the sender and intended recipient have consented to the interception;

- Provided for the Secretary of State to authorise interception in certain limited circumstances, by means of warrants issued to organisations such as the security and intelligence agencies and the police.

Section 4 of RIPA 2000 provided for the Secretary of State to make regulations authorising businesses to intercept for certain evidential purposes. The government achieved this through the *Lawful Business Practice Regulations*, which came into effect on 24 October 2000.

### 5.5.2 *Lawful Business Practice Regulations*: undermining data protection?

The *Lawful Business Practice Regulations* permitted businesses to intercept communications without consent for the following purposes:

- To establish the existence of facts;
- To ascertain compliance with regulatory or self-regulatory practices or procedures (quality control);
- To ascertain or demonstrate standards which are or ought to be achieved (training);
- To prevent or detect crime;
- To investigate or detect unauthorised use of telecommunication systems;
- To ensure effective system operation (for example, by monitoring for viruses).

Additionally, communications could be monitored to determine whether or not they were business communications. The wide scope of the *Regulations* led many in the media and campaign groups to question whether they undermined the provisions of the DPA 1998. To quote Akdeniz from the Internet civil liberties group, Cyber Rights-Cyber Liberties, the vagueness of the Regulations meant that "anything is justified under them" [85]. At the same time that the *Regulations* were being finalised, the OIC released its draft *Employment Code of Practice* (discussed in detail in Chapter 4, section 4.6.3) resulting in what many perceived to be a confused legal environment[86].

The OIC, defending its *Draft Code of Practice*, strongly emphasised that the *Regulations* only addressed the act of interception[87]. They did not address the monitoring of traffic data, nor did they deal with the storage and use of personal information obtained as a result of interception. Monitoring needed to be conducted in accordance with the requirements of the DPA 1998. By its very nature, monitoring will involve personal data that must be obtained and processed in such a way that it is both lawful and fair to employees. Taken to its logical conclusion, an employer who acquires information by surveillance under the *Regulations* could still be prosecuted under the DPA 1998. This has sparked

criticism from the Confederation of British Industry that the draft *Code* did not adequately meet the needs of employers[88]. Additionally, any monitoring must:

- Be necessary;
- Be proportionate to achieving the business purpose (doing no more than needs to be done);
- Respect the privacy of individuals.

If audit logs, or similar, were being applied to track websites or email addresses used by employees, the resulting records - if they identified individuals – would contain personal data for the purposes of the DPA 1998. An employee would be entitled to seek, and could expect to be given, access under section 7 of that Act, unless one of the exceptions could be invoked. It is unlikely that third parties would be entitled to see the log.

Employers were advised to limit monitoring to traffic data - rather than the contents of communications - should that achieve their business requirements. If the traffic record alone was insufficient, organisations were to use it to ensure any further monitoring should be, as far as possible, strictly limited and targeted. If employers were monitoring the content of incoming emails to detect computer viruses, usage of an automated monitoring and detection process was advised. A need for virus detection did not warrant reading the content of incoming emails. Ultimately, RIPA 2000 has to be interpreted by judges within the context of the HRA 1998 - with its own in-built conflict between Article 8 right to privacy, and Article 10 freedom of expression.

### 5.5.3 Anti-Terrorism, Crime and Security Act (ATCSA) 2001

Since the terrorist attacks on the US on 11 September 2001, a number of Western governments have passed anti-terrorism measures. In December 2001, the UK government enacted the ATCSA 2001. In Chapter 3 (section 3.3), the views of lawyers and journalists concerning the data protection implications – and the costs to industry - of this Act were considered. This subsection will look in a little more

detail at some of the provisions of ATCSA 2001, in particular, how the Act interfaces with the DPA 1998 and HRA 1998 – and any problems public organisations may face.

*Provisions affecting data protection*

According to the Home Office, the purpose of ATCSA 2001 is 'to enhance our anti-terrorism and security capability'. The Act is wide-ranging, structured in 14 parts and eight schedules. It includes: measures tackling terrorist finance; the streamlining of immigration procedures; provisions against inciting religious hatred or violence; improving civil nuclear security; extension of police powers; and, under Part 11, retention of communications data. It is the provisions under Part 11 that impact is greatest on data protection.

In this context – as in RIPA 2000 (section 21) – communications data means traffic data and any other data which are not part of the actual communications themselves. This is essentially billing data, subscriber data, details of numbers dialled or Internet sites accessed by a given subscriber, email headers and so on. It does not include, for example, the contents of email messages or voice calls. The data is to be retained by communications providers – such as internet service providers (ISPs) – for national security purposes, so that they can be accessed by the security, intelligence and law enforcement agencies by means of a voluntary code of practice. This code is to be drawn up in consultation with industry, law enforcement agencies and the OIC. This process is currently underway and a final version of the voluntary code is expected during 2003.

However, should the Secretary of State not be satisfied with the operation of the voluntary code, he is permitted under section 104 of the Act to issue compulsory directions on communications service providers. There is no need to consult with the OIC over such an order, over the content of which the Secretary of State enjoys a substantial amount of discretion. However, if this power is not renewed within two years of the enactment of the Act, it will lapse.

Concerns have been expressed that this Act undermines the DPA 1998 and the HRA 1998. In a press release promoting the publication of her second annual report in July 2002, the Information Commissioner stated the retention of communications data by service providers is 'of continuing concern'[89]. The Commissioner continued that, whilst the purpose for which data could be retained was limited to matters of national security, the basis on which law enforcement bodies could have access to those communications had not been similarly restricted. This meant that the data could be accessed for any of the wider law enforcement activities provided for in RIPA 2000. Such activities include not just the prevention and detection of crime, but also matters relating to public health and tax collection. Essentially, the data may not be used for the purposes for which it was collected – a clear breach of Principle Two of the DPA 1998.

Secondly, if there is a need to retain the data for longer than the communications provider would for their own purposes in order to prevent and detect crime then a statutory duty to retain would have to be established. This would ensure that the DPA 1998 (Principle Five) is not contravened. This approach should have been adopted at the enactment of the Act, rather than being left as an alternative to be considered at a later date, as it would have provided a proper legal basis for processing by the communications provider.

Additionally, concerns have been raised by the OIC and lawyers about the interface of the proposed legislation with the ECHR rights. The absence of clarity concerning the Secretary of State's powers to issue a code of practice concerning data retention has been questioned. Although Article 8 (2) of the ECHR permits interference with individual privacy 'in accordance with the law', the Convention further requires that the law concerned must be accessible and precise – that is, foreseeable in its consequences[90]. According to Strasbourg case law[91], Article 8 requires a positive framework of legal rules circumscribing the exercise of any such power, and incorporating legally binding safeguards against abuse. The law must indicate the circumstances in which such interference can occur, its duration and the limits of the authorities' powers. Without any sight of the proposed code of practice or any secondary legislation proposed under the Act, it is not possible to assess the legal framework in this area. Therefore, the legislation appears to be

incompatible with Convention rights as it fails the requirement for precision and foreseeability in the delineation of the Secretary of State's powers.

## 5.6 Conclusions

This Chapter has given insight into the complexity of the wider legal environment surrounding and impacting on privacy of personal information. Considerable legal changes have been enacted in both Europe and UK since the enactment of the DPA 1998. Some observations are outlined below:

(i) The competing legal demands on public organisations.

This has been clear, particularly over the last five or six years. On the one hand, the UK government is acting to incorporate effective privacy standards into data handling through the implementation of the DPA 1998 and the HRA 1998. On the other hand, more recent legislation such as RIPA 2000 and ATSCA 2001 have shifted the emphasis towards sharing of personal information with other public organisations. Concerns about the privacy implications of recent laws regarding interception and retention of communications data have been expressed by lawyers and the OIC. Finally, the complex legislative environment places competing pressures on those attempting to achieve data protection compliance.

(ii) The need for more explicit case law.

Although the laws analysed in this Chapter have some explicit provisions, many of the finer details of the statutes – particularly the extent to which a culture of protecting personal data can be established in public organisations – will need be determined by the courts on a case-by-case basis. In particular, the impact of the HRA 1998 – incorporating a set of principles into UK law - will take years to assess. Although the *Robertson* case was significant, the majority of case study interviewees perceived the HRA 1998 as having little direct impact on the information handling processes of public authorities. To quote one Data Protection Officer, public organisations were maintaining a "watching brief"[92].

(iii) The impact of FOIA 2000.

Of the laws analysed in this Chapter, FOIA 2000 will have the most tangible effect on the daily work of organisational Data Protection Officers (DPOs). As quoted in subsection 5.4.4, some interviewees viewed the FOIA 2000 as a tidying-up exercise, ensuring that public sector records management practices were better coordinated. Certainly, the Act expanded the scope of the DPA 1998 to cover 'unstructured' manual data. More practically, it increased the workload of public authorities with many organisations currently drafting publication schemes, auditing records and preparing job descriptions for new personnel. The impact of FOIA 2000 on the role of DPOs will be considered in Chapters 6 and 7.

(iv) The need for a strong lead from the OIC.

This finding has been implicit throughout both Chapters 4 and 5. Whilst the conclusions to the previous Chapter made it clear that the OIC faced many difficulties in promoting data protection compliance, there is little doubt that the supervisory authority has an important role to play. With the Information Commissioner now responsible for overseeing and enforcing *both* data protection and freedom of information, a strong lead is essential. To date, the OIC has been very positive in this regard – maintaining a high profile and commenting on the legal issues discussed in this Chapter. Moreover, public organisations implementing the legislation must be able to refer to the OIC for immediate and consistent advice. Fieldwork in Chapters 6 and 7 will show that this was not always the case. Finally, the public must be informed of their access rights under both the DPA 1998 and the FOIA 2000. A process of education, already underway with some success[93], needs to be continued and expanded so that individuals are fully aware of their rights under the new Acts.

## References and Notes

[1] United Nations. *Universal Declaration of Human Rights 1948.* Article 12.

[2] *Ibid.*

[3] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, ETS no. 108. Strasbourg, 1981. Explanatory report, para. 19.

[4] European Communities. Commission. *Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.* Official Journal of the European Communities. No. L281/31 (23/11/95). See recitals 1 and 2.

[5] For full list of rights and freedoms refer:

- Council of Europe. *Convention for the protection of Human Rights and Fundamental Freedoms.* Article 8. ETS no. 005. Rome, 1950.

[6] Only a person considered a victim can bring proceedings against a public authority under the HRA 1998. A victim is someone who is directly affected by the act in question. This can include companies as well as individuals. Additionally, a victim may also be a person who is at risk of being directly affected by a measure. Organisations, interest groups and trade unions cannot bring a case unless they themselves are victims. However, they can provide legal or other assistance to a victim. Governmental organisations, such as local authorities, cannot be victims.

[7] The referencing of most of the cases quoted in this chapter takes after:

- Wadham, J. and H. Mountfield, *Human Rights Act 1998*, 1999.

'EHRR' refers to *European Human Rights Reports*, the best UK source for decisions of the European Court of Human Rights – publishing full judgements of significant cases. For example, in '1976, 2 EHRR 1': '1976' refers to the year of the decision; '2' to the volume of EHRR; and '1' to the page number where the decision can be found.

Those not included in EHRR are referenced by their application number. This comprises a five digit number followed by the year of application, and then the date of decision. For an example, see *Rotaru v Romania,* ref. 16.

[8] Prior to this, complaints could have been heard by the European Commission on Human Rights. This body was abolished with the introduction of Protocol 11 to the ECHR on 1 November 1998.

[9] Approximately 95 per cent of applications are found to be inadmissible. Source:

- Wadham, J. and H. Mountfield, ref. 7, pp.142-143.

[10] *Convention for the protection of Human Rights and Fundamental Freedoms.* ref. 5, Article 8.

[11] Wadham, J. and H. Mountfield, ref. 7, pp.91-96.

[12] *Ibid.*, p.92.

[13] Williams, K. Re-regulating free speech: privilege, public interest and privacy. *Web Journal of Current Legal Issues*, 1999, 1. URL: http://webjcli.ncl.ac.uk/1999/issue1/williams1.html [Accessed 16/01/03].

[14] For full discussion of the background to the addition of section 12 to the HRA, refer to:

- Singh, R. Privacy and the media after the Human Rights Act. *European Human Rights Law Review*, 1998, 6, pp. 712-729.

[15] Jay, R. UK Data Protection Act 1998 - the Human Rights context. *International Review of Law Computers and Technology*, 2000, 14 (3), 388.

[16] *Rotaru v Romania* (2000). Application No. 28341/95, 4 May 2000.

[17] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, ref. 3, Article 1.

[18] Wadham, J. and H. Mountfield, ref. 7, p.24.

[19] Jay, R., ref. 15, 390.

[20] BBC News Online. Forum: Human Rights Act - Quiz Lord Lester. *BBC News Online.* 06/10/00. URL: http://newsvote.bbc.co.uk/low/english/talking_point/forum/newsid_954000/954831.stm [Accessed 16/01/03].

[21] This is made explicit in the long title of the HRA:

> 'An Act to *give further effect* to rights and freedoms guaranteed under the European Convention on Human Rights; to make provision with respect to holders of certain judicial offices who become judges in the European Court of Human Rights; and for connected purposes.' (My italics).

[22] Lord Irvine of Lairg. House of Lords, Report Stage. *Hansard HL*, 585 (column 421) 29 January 1998.

[23] See Singh, R., ref. 14.

[24] See Palmer, S. Human rights: implications for labour law. *Cambridge Law Journal*, 2000, 59 (1), 168-200.

[25] Gearty, C. Incorporation of the European Convention on Human Rights; some guesses about the future in Butler, F. (ed.) *Human rights for the new millennium*. Kluwer Law International, 2000, pp.33-47.

[26] Jay, R., ref. 15, p.395.

[27] The legal system in Scotland differs slightly from England and Wales, taking more of a civil law – rather than case law – approach.

[28] Kearns, P. Privacy and the Human Rights Act 1998. *New Law Journal*, 16/03/01, 377-8.

[29] *Ibid.*, p.377.

[30] Owing to the celebrity status of those involved, the case received substantial publicity at the time. For a full analysis of this case refer:

- Thomas, S. Privacy: media. *Privacy and Data Protection*, 2001, 1 (3), 8-9.

[31] Kearns, ref 28., p.378.

[32] Great Britain. *Representation of the People Act 2000*. London: TSO, s.9.

[33] For analysis of the chronology of *Robertson* in relation to the Representation of the People Act 2000, refer to the following policy paper:

- Great Britain. Department for Transport, Local Government and the Regions. *Electoral Registers – Access, Supply and Sale*. May 2002. URL: http://www.lcd.gov.uk/consult/elections/pdf/policypaper.pdf [Accessed 07/05/03].

[34] Protocol 1, Article 3 of the ECHR guarantees the right to free elections. This provision was incorporated into the HRA 1998.

[35] Refer:

- Great Britain. *Representation of the People (England and Wales) (Amendment) Regulations 2002*. Statutory Instrument 2002, No. 1871. TSO, 2002. URL: http://www.hmso.gov.uk/si/si2002/20021871.htm [Accessed 16/01/03].

[36] These uses are electoral purposes, investigation of crime and credit checks.

[37] Privacy and Data Protection. Robertson commences new action against local authority. *Privacy and Data Protection*, 2002, 3 (1), 16.

[38] Privacy and Data Protection. Naomi Campbell wins damages in landmark privacy ruling. *Privacy and Data Protection*, 2002, 2 (5), 1, 13.

[39] Broadly, section 32 of the DPA 1998 permits the publication of personal data for journalistic purposes which are considered to be in the public interest. In the first instance decision, Morland interpreted the provisions of section 32 as relating to processing of personal data *prior* to publication only. In the Court of Appeal, the judges went against this – stating that section 32 of the DPA 1998 applied both before and *after* publication, as it would be illogical for the data controller to be obliged to comply with the provisions of the Act until the moment of publication but not thereafter. For further analysis, refer:

- Harper, L. Model behaviour. *Privacy and Data Protection*, 2002, 3 (2), 8-9.

[40] Great Britain. Home Office: Human Rights Unit. *Human Rights Act: Core guidance for public authorities: a new era of rights and responsibilities*, 2000. URL: http://www.lcd.gov.uk/hract/coregd.htm [Accessed 16/01/03].

[41] Great Britain. Home Office: Human Rights Unit. *Human Rights Act 1998: Guidance for Departments*. 2nd edition, 2000. URL: http://www.lcd.gov.uk/hract/guidance.htm [Accessed 16/01/03].

[42] Great Britain. Lord Chancellor's Department. *Study Guide – Human Rights Act.* 2nd edition, 2002. URL: http://www.lcd.gov.uk/hract/studyguide/index.htm [Accessed 16/01/03].

[43] For further details, refer URL: http://www.lcd.gov.uk/hract/studyguide/index.htm [Accessed 16/01/03].

[44] Pleming, N. Assessing the Act: a firm foundation or a false start? *European Human Rights Law Review*, 2000, 6, 560-579.

[45] Refer URL: http://www.parliament.uk/commons/selcom/hrhome.htm [Accessed 16/01/03].

[46] Great Britain. District Audit. *The Human Rights Act: a bulletin for public bodies.* 2002. URL: http://www.district-audit.gov.uk/PDF/district-audit-humanrights-02.pdf [Accessed 16/01/03].

[47] Wadham, J. and H. Mountfield, ref. 7, pp.97-98.

[48] Burnes, C. Human rights in employment. *Privacy and Data Protection*, 2000 1 (2), 4-5.

[49] Rawstorne, T. Bosses can sack staff over emails. *The Daily Mail*, 2000 pp.1-2.

[50] Banisar, D. Freedom of Information and access to government records around the world. Privacy International, 2002. URL: http://www.freedominfo.org/survey/ [Accessed 16/01/03].

[51] Wood, S. and J. Dearnley. Open government? Freedom of information legislation and information provision in the UK. *Proceedings of 8th International BOBCATSSS Symposium on Library and Information Science, Krakow, Poland.* 24-26 January 2000, p.309.

[52] Interview with Alain Brun, DG Internal Market, European Commission, Brussels. 6 July 1999.

[53] Sweden, along with Finland and Austria, acceded to the EU on 01/01/95.

[54] *Directive 95/46/EC*, ref. 4, recital 72.

[55] Refer URL: European Communities. *Treaty on European Union.* Maastricht, 1992. For full text, refer: http://europa.eu.int/en/record/mt/top.html [Accessed 16/01/03].

[56] For details, refer to *The Amsterdam Treaty: a comprehensive guide.* URL: http://europa.eu.int/scadplus/leg/en/lvb/a21000.htm [Accessed 16/01/03].

[57] European Communities. Commission. *Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents*. Official Journal of the European Communities. No. L 145/43. (31/05/2001). URL: http://europa.eu.int/comm/secretariat_general/sgc/acc_doc/index_en.htm [Accessed 16/01/03].

[58] Great Britain. Cabinet Office. *Open Government*. HMSO, 1979. (Cmnd 7520).

[59] Great Britain. *Local Government (Access to Information) Act 1985*. London: HMSO.

[60] Great Britain. *Access to Medical Reports Act 1988*. London: HMSO.

[61] Great Britain. Cabinet Office. *Open Government*. London: HMSO, 1993. (Cmnd 2290).

[62] Wood, S. and J. Dearnley, ref. 51, 310-311.

[63] For example, the Department of Trade and Industry's refusal to release a summary of information on encryption, criticised in:

- Great Britain. House of Commons. *The Parliamentary Ombudsman Annual Report 1999-2000*, HMSO, 2000. (HC 593). pp. 44-46.

[64] Great Britain. House of Commons. Select Committee on the Parliamentary Commissioner for Administration. *Second special report on open government*. HMSO, 1996. (HC 1995-1996 556).

[65] Great Britain. Cabinet Office. *Your right to know: the government's proposals for a Freedom of Information Act*. HMSO, 1997. (Cmnd 3818).

[66] Campaign for Freedom of Information. Press release. *Deeply disappointing Information Bill 'weaker than Conservatives' openness code'*. 24/05/99. URL: http://www.cfoi.org.uk/draftbill240599pr.html [Accessed 16/01/03].

[67] Amendments prior to the Lords Committee stage appeared on the Parliament website on 31/07/00. Refer:

- Great Britain. Houses of Parliament. Session 1999-2000. *Freedom of Information Bill – amendments to be debated in the House of Lords*. 31/07/00. URL:

http://www.publications.parliament.uk/pa/ld199900/ldbills/055/amend/am055-p.htm (Accessed 14/05/03).

[68] The amendment became section 2 (2) of the Act:

> 'In respect of any information which is exempt information [the duty to disclose] does not apply if or to the extent that –
> (b) in all circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.'

The significance of this amendment was the subject of some controversy, with campaigners and even the Liberal Democrat spokesman, Lord Goodhart, claiming it would not make much of a difference. For opinion and further analysis, refer:

- Campaign for Freedom of Information. Press release. *Anger at Liberal Democrat decision to back flawed Information Bill.* 13/11/00. URL: http://www.cfoi.org.uk/libdems131100pr.html [Accessed 14/05/03].
- Cornford, T. The Freedom of Information Act 2000: genuine or sham? *Web Journal of Current Legal Issues.* 2001 (3). URL: http://webjcli.ncl.ac.uk/2001/issue3/cornford3.html [Accessed 14/05/03].

[69] Wadham, J., J. Griffiths and B. Rigby. *Freedom of Information Act 2000*, 2001. p.ix.

[70] Refer:

- Great Britain. Office of the Information Commissioner. *Freedom of Information Act 2000: An overview*, January 2002, pp.6-7. URL: http://www.dataprotection.gov.uk/dpr/foi.nsf (Under 'General Information') [Accessed 16/01/03].

[71] For full list: *Ibid.*, pp. 6-7.

[72] For example, refer:

- Campaign for Freedom of Information. FOI Bill: Lords Third Reading Briefing. 21/11/00. URL: http://www.cfoi.org.uk/newin00.html [Accessed 16/01/03].

[73] The Earl of Northesk. House of Lords. Committee Stage. *Hansard HL*, 618 (column 431) 25 October 2000.

[74] The Fees Regulations are still at draft stage. Refer:

- Great Britain. Lord Chancellor's Department. *Annual report on bringing fully into force those provisions of the Freedom of Information Act 2000 which are not yet fully in force.* 2002. (HC6).

[75] Campaign for Freedom of Information. *Government to abandon freedom of information timetable?* 02/11/01. URL: http://www.cfoi.org.uk/newin01.html [Accessed 16/01/03].

[76] Hencke, D. and R. Evans. Blair wins battle to put open government on ice. *The Guardian*, 30/10/01. URL: http://www.guardian.co.uk/Archive/Article/0,4273,4287729,00.html [Accessed 16/01/03].

[77] Great Britain. Lord Chancellor's Department. *Annual report on proposals for bringing fully into force those provisions of the Freedom of Information Act 2000 which are not yet fully in force.* Lord Chancellor's Department, November 2001. (HC 367). URL: http://www.lcd.gov.uk/foi/imprep/annrep01.htm [Accessed 16/01/03].

[78] Campaign for Freedom of Information. *Double blow for FOI*, 13/11/01. URL: http://www.cfoi.org.uk/newin01.html [Accessed 16/01/03].

[79] The timetable for publication schemes include: most of central government (November 2002); local authorities (February 2003); police (June 2003); NHS (October 2003); schools and universities (February 2004). Source: Office of the Information Commissioner, URL: http://www.dataprotection.gov.uk/dpr/foi.nsf [Accessed 16/01/03].

[80] Great Britain. *Freedom of Information (Scotland) Act 2002.* London: TSO.

[81] Interview with Maurice Frankel, Campaign for Freedom of Information, London. 7 November 2001.

[82] *Freedom of Information (Scotland) Act 2002.* ref. 80, s.75.

[83] For details of guidance issued by Lord Chancellor's Department, refer URL: http://www.lcd.gov.uk/foi/foidpunit.htm [Accessed 16/01/03].

[84] For details of OIC guidance, refer URL: http://www.dataprotection.gov.uk/dpr/foi.nsf [Accessed 16/01/03].

[85] Thompson, B. Every click you make. Online. *The Guardian,* 2 November 2000 pp. 2-3.

[86] *Ibid.*

[87] Refer to:

- Great Britain. Office of the Data Protection Commissioner. *Draft Code of Practice: The use of personal data in employer/employee relationships*, 2000, pp. 25-34.
  URL: http://www.dataprotection.gov.uk/dpr/dpdoc.nsf [Accessed 16/01/03].

[88] Thompson, B. ref. 85, p.3.

[89] Great Britain. Office of the Information Commissioner. News release. Monitoring must be justified. *Office of the Information Commissioner*, 10/07/02.
URL: http://www.dataprotection.gov.uk/dpr/dpdoc1.nsf [Accessed 16/01/03].

[90] For further discussion of this point, refer to Wadham and Mountfield, ref. 7, pp.12-13. The authors cite the following case law to support their views:

- *Sunday Times v United Kingdom* (1979) 2 EHRR 245;
- *Malone v United Kingdom* (1984) 7 EHRR 14;
- *Halford v United Kingdom* (1997) 24 EHRR 523.

[91] *Ibid.*

[92] Refer case study analysis, Chapter 7.

[93] Refer:

- Great Britain. Office of the Data Protection Commissioner. *Annual Report and Accounts for the year ending 31 March 2002*, 2002, p.74.

# 6. Findings: questionnaire survey and expert interviews

Following discussion of the literature, coupled with scrutiny of the laws impacting on data protection compliance in public organisations, this Chapter marks the point of departure for analysis of fieldwork. The methodology behind the techniques chosen was discussed in detail in Chapter 2. This Chapter is divided into two discrete sections. Section 6.1 considers 14 of the 15 interviews conducted with experts in the fields of policy-making, law and campaigning. Concerns raised by interviewees include:

- The "convoluted" text of the UK DPA 1998;
- Data protection in the employment context;
- The development of data protection policy within organisations;
- The impact of related legislation on information privacy – in particular, UK statutes relating to freedom of information, human rights and anti-terrorism.

The findings triangulate the conclusions drawn in previous, desk research, Chapters. The outstanding interview, with Sir Norman Lindop, chairman of the Data Protection Committee 1976-1978, is unique in providing historical context to data protection in the UK. Consequently, it is analysed separately in Appendix A.

Section 6.2 of this Chapter examines findings from the questionnaire survey comprising almost 400 public organisations. For the reasons stated in Chapter 2, the questionnaire focused on employee personal data. Data analysed include:

- Measures to ensure compliance with the DPA 1998;
- Subject access procedures for employees;
- Security procedures for safeguarding employee records;
- Monitoring of workplace email and internet use;
- Awareness and opinion concerning various legislation and the *Employment Practices Data Protection Code*.

Some of the survey produced findings – particularly in the fields of staff training and formation of policies – that were pursued during case study interviews. These are analysed in Chapter 7.

## 6.1 Expert interviews

This section presents detailed findings from the expert interviews. The interviews were conducted to establish an overview of policy and expert opinion concerning data protection and related issues. The interviews triangulated desk research and questionnaire findings, and raised issues that were later explored during the case study interviews.

In total, 15 people from a variety of organisations involved in law, policy-making and campaigning were interviewed. Only individuals who gave permission are named in this thesis. In all other instances the organisation they represented has been referred to. The participants are listed below:

- Sir Norman Lindop, chairman of the Data Protection Committee 1976-1978;
- Data Protection Unit, DG Internal Market, European Commission;
- Office of the Information Commissioner (OIC);
- Lord Chancellor's Department;
- Office of the e-Envoy (Oe-E), Cabinet Office;

- Professor David Feldman, Joint Committee on Human Rights, Houses of Parliament;
- European Union Committee, House of Lords, Houses of Parliament;
- Union of Industrial and Employers' Confederations of Europe (UNICE);
- Confederation of British Industry (CBI);
- Hannah Reed, Trades Union Congress (TUC);

- Manufacturing, Science and Finance Union - Information Technology Professionals Association (MSF-ITPA, abbreviated in this text to 'MSF');
- JUSTICE;
- Consumers' International (CI);
- Campaign for Freedom of Information (CFOI);
- Hazel Grant, Bird and Bird, international law firm.

The questions were tailored to the expertise of individual interviewees. The interview with Lindop was unique in that it focused almost exclusively on the history behind UK data protection legislation. As stated earlier, analysis of this interview has consequently been placed in Appendix A. However, the discussions with Lindop were referred to in Chapter 4 (section 4.5), detailing context to the UK Data Protection Acts 1984 and 1998. The remaining 14 interviews included the following common issues:

- Interviewee's role in their particular organisation;
- Aims of the organisation;
- When and how that organisation developed an interest in data protection and/or human rights;
- Level of data protection and/or human rights expertise in the organisation;
- Other bodies consulted/extent of peer group cooperation within this field;
- Official and personal opinion on legislation and official guidance, especially:
  - Text of the various Acts (DPA 1998; HRA 1998; FOIA 2000; RIPA 2000);
  - Workability of official guidance in this field (for example, *Employment Practices Data Protection Code*);
  - Recommendations for improvement.
- Research and policy work conducted in this field;
- Future challenges facing organisations concerning data protection and human rights.

It should be noted that 13 of the interviews were conducted in the two months following the terrorist attacks in the US on 11 September 2001. Hence, anti-terrorism measures – particularly relating to the retention of personal data – suddenly became prominent for those working with data protection issues. Many of the topics relating to data protection in this section have been discussed to some extent in Chapter 4. However, the interviewees added fresh insights based on their personal experiences. This section analyses textual difficulties presented by the DPA 1998, employment practices, the transfer of personal data to third countries, and the need for organisations to have clear data protection policies. Additionally, the interface between data protection and other concerns such as HRA 1998, FOIA 2000 and the various anti-terrorist measures proposed during autumn 2001 are considered. Finally, conclusions are drawn, summarising the key findings from the expert interviews.

### 6.1.1 Data Protection Act 1998

The complexity of the UK DPA 1998 was raised in a number of interviews. According to the majority of interviewees, this strengthened the need for clear and practical guidance, from the European Commission as the institution responsible for the underlying Directive 95/46/EC as well as from UK government and the OIC. The need for further clarity has been recognised and gradually addressed through the documents of the EU Article 29 Data Protection Working Party[1] and the OIC's publication of two *Codes of Practice*[2].

The text of the DPA 1998 was subjected to heavy criticism, being described as "appallingly drafted" and "ambiguous". The Lord Chancellor's Department – the government department responsible for data protection and freedom of information since June 2001 – is in the process of appraising the DPA 1998. Completion of the appraisal has been deferred until the European Commission publishes its report on the implementation of Directive 95/46/EC. Nevertheless, responses to the Department's consultation exercise were published in December 2001[3]. Key issues identified by respondents included:

- Definition problems – in particular, the lack of definition for 'consent';
- Confusion over international data transfers to third countries;
- Unclear relationship between 'data controller' and 'data processor', causing particular difficulties for large organisations such as the NHS and multi-nationals;
- Problems of interpretation over the 'sensitive data' distinction, with the OIC suggesting it should be abandoned.

Grant, a lawyer at Bird and Bird aiding organisations in IT procurement and data protection, stated that clients experienced difficulties with terms used in the Act. Speaking in a personal capacity, Grant criticised the text of the Act as "convoluted", with too much guidance around a few words such as "structured filing system"[4]. Its ambiguity was also censured, supporting the observations identified during the Lord Chancellor's consultation exercise. In addition to the issues surrounding consent and relationships between data controllers and data processors, the meaning of terms such as 'personal data', 'adequate protection' and 'disproportionate effort' were also far from clear. Finally, the conditions for fair and lawful processing of personal data set out in Schedules 2 and 3 of the Act were indistinct – in particular Schedule 2 (6) which permitted processing that was in the 'legitimate interests pursued by the data controller'. Grant's comment relating to that condition summed up the attitude of many case study organisations to the whole Act:

> "We don't really know how far that will extend until we've had several years worth of guidance on it."[5]

Guidance relating to employment practices is discussed in the next subsection.

### 6.1.2 Employment practices

This subsection focuses on protection of employee personal data, adding to the perspectives given in Chapter 4 (section 4.6). This issue is analysed at three levels:

- Possible EU moves towards legislation;
- Opinion concerning the OIC's *Employment Practices Data Protection Code*;
- Collective agreements being drafted at a local level between employers and trade unions.

*EU working paper and possible moves toward legislation*

In September 2001, an interview was conducted at the Data Protection Unit, based in DG Internal Market, part of the European Commission. During the meeting, a recently drafted working paper concerning data protection in the employment environment was discussed[6]. This paper, which the interviewee had contributed to, was published by the Article 29 committee. The aim of this paper was to provide guidance for organisations, to clarify certain aspects of the application of Directive 95/46/EC in the employment context. Its key points were:

- Most employment activities were within the scope of Directive 95/46/EC;
- Employers needed to consider fundamental data protection principles when processing personal data belonging to employees;
- As the relationship between employer and employee is not an equal one, reliance on employee consent should be limited.

It bore many similarities to the OIC's *Draft Code of Practice: The use of personal data in employer/employee relationships*[7], and it was no surprise to learn that David Smith, Assistant Information Commissioner at the OIC, had a leading role in its drafting. Such EU working papers were described by the interviewee at the EU Data Protection Unit as "soft law"[8], as only the national supervisory authorities were bound by its provisions. However, given that the supervisory authorities applied Directive 95/46/EC via national data protection laws, the effect was clear. If those authorities stated that employee consent was weak, "it will impact on national policies"[9]. Speaking in a personal capacity, the interviewee believed action by the European Commission in this field was likely in the course

of 2002, although some delays were expected following the terrorist attacks in the US on 11 September 2001:

> "As you know, Article 30 states one of the tasks of the Working Party is to promote the harmonisation of national law[10]. So we should start by this. If this is not sufficient maybe we should consider supplementary action. This opinion is the foundation...that is my personal view."[11]

The European Employers' Confederation (UNICE) had argued against centralised EU legislation concerning workers' personal data following an initial EU consultation in autumn 2001[12]. The employers' organisation stated that existing regulations – particularly Directive 95/46/EC – applied to workers' personal data and that specific solutions could be found at a more decentralised level, for example, through codes of practice, self-regulation, and voluntary agreements:

> 'social partners at national level would be in a better position to address problems as and when identified.'[13]

In a written answer to interview questions for this thesis given in December 2001, UNICE stated that employees did have a right to some privacy in the workplace, 'but privacy can have some limitations in the employment context'[14]. For example, some controls may be necessary to ensure that the company's IT system is not used to send offensive or illegal material. Such systems were perfectly acceptable, 'provided the employee is informed that control systems are in place'[15].

Notwithstanding such reservations, the European Commission launched a second stage consultation on the protection of workers' personal data[16]. Given the more general nature of Directive 95/46/EC, the Commission believed there was a need for "clearer, simpler rules on the protection of workers' personal data which take better account of the employer/worker relationship"[17]. The substance of the second consultation covered:

- Consent;

- Access to, and processing of, medical data;
- Drug testing and genetic testing;
- Monitoring and surveillance.

Although acknowledging that some of these measures had been tackled by member states through national legislation and various codes of practice, the Commission argued that different treatment of workers' personal data within the EU may create barriers to the free movement of information within the internal market[18].

UNICE, and other 'social partners' – including trade union and consumer representatives – had six weeks from 31 October 2002 to comment on the Commission's proposals, or decide to take up the matter themselves, independently of the Commission, with a view to establishing their own EU-wide initiative in this area[19]. UNICE replied in January 2003, stating their opposition to the Commission's proposal, and to opening negotiations with other social partners[20]. The employer's organisation repeated their arguments given in response to the first stage consultation. Firstly, directives such as 95/46/EC afforded a high degree of protection to European workers. Secondly, the Commission's own assessment own report on the implementation of Directive 95/46/EC has yet to be published. Finally, that the Article 29 committee is the appropriate forum for such discussions.

*UK code of practice*

During interviews with organisations based in the UK, the *Draft Code of Practice: The use of personal data in employer/employee relationships* was frequently discussed. A strategic policy officer interviewed at the OIC stated that the UK was one of the first EU member states to produce a code of practice in this field. The OIC guidance was "not an increased obligation, [but] reaffirmed existing obligations"[21]. The interviewee agreed there had been confusion over what constituted 'consent' under the DPA 1998 and both employers and employees had requested further clarification. Acknowledging that the first draft of the *Code* had been "badly presented", the interviewee stated "the main thrust of the final version

is going to remain the same – especially the issue of monitoring in the workplace"[22].

Indeed, the draft *Code* had been criticised by many organisations. Grant described the draft as "totally unworkable"[23]. It was too lengthy at 60-plus pages. The new *Code* – which will be published in four separate parts – is "now going to be a quite incredible length, it's going to be over 200 pages"[24]. This may be useful, Grant concurred, for large organisations such as Marks and Spencer and the NHS, the chances of anyone in small organisations reading it at all are "very slim". Additionally, Grant contested the position the OIC has adopted in the *Code* limiting the reliance on consent:

> "There are few other means available. In recording sensitive personal data, how else are they going to do it?"[25]

Finally, concern was raised that in the *Code*, the OIC has incorporated their interpretation of the law with their suggestions for good practice. Thus, there is a risk of "scope-creep":

> "The law will increase, because what will happen is if big employers follow the Code to the letter, then that will become normal practice in personnel departments."[26]

Therefore, Grant contested, the *Code* will "push out the boundaries of the Act"[27].

The CBI adopted a broadly similar view. On the issue of timing, the draft *Code* - when published in October 2000 – attempted to anticipate the provisions of the *Lawful Business Practice Regulations* (*LBPR*) finalised in the same month. In the end, the draft *Code* "completely contradicted the Regulations, which didn't help the consultation process"[28]. Delaying the release of the draft *Code* for a few weeks "could have saved a lot of confusion", and improved coordination between the Department of Trade and Industry and the OIC.

However, both employee representatives – the TUC and the Manufacturing, Science and Finance Union (MSF) – broadly welcomed the draft *Code*. To quote the interviewee at the latter organisation:

> "We've been supportive of the principle of a data protection code as envisaged by the Information Commissioner, and have been pushing for such a *Code*"[29].

The interviewee viewed some of the arguments by employers in favour of monitoring as ill thought through. Most legitimate interests of employers could be achieved through "means other than monitoring and surveillance"[30]. For example, one of the organisations the MSF works with attempts to safeguard against downloading pornography by limiting the size of file that can be attached to an email to half a megabyte, "about 30 pages of A4"[31]. Should the employee require a larger attachment, they need to get express permission.

Reed, from the TUC, also welcomed the approach taken in the draft *Code*:

> "Our viewpoint is that the code of practice should be detailed and should also have wide-ranging guidance."[32]

The interviewee pointed out that TUC had wide experience of working with ACAS[33] and equal opportunities codes of practice, and employers, too, had worked with codes of practice. As quoted in Chapter 4 (section 4.6.3), Reed emphasised that the draft *Code* was there to aid employers in creating policies – and avoiding litigation – in what is a complicated and sometimes controversial field of law. Reed was concerned that the final version was going to be "watered down", which, for the reasons give above, would "not necessarily be much help to employers". Finally, Reed noted that the draft *Code* referred to 'employees' in the employment relationship whilst Directive 95/46/EC actually relates to 'workers'. Under this distinction, most agency and casual staff would be excluded from the interpretations outlined in the draft *Code*.

*Towards collective agreements?*

In general, the TUC and MSF welcomed the extended protection afforded by the DPA 1998, but acknowledged that the provisions of the Act could lead to very rigid systems of filing and monitoring and "everyone could get themselves tied up in bureaucracy"[34]. The problem with the DPA 1998, according to Reed, was a lack of awareness among organisations concerning the scope of data protection – which extended beyond correction, deletion and access to interview notes. Indeed, the Act also "covers things such as drug-testing and alcohol testing"[35].

In terms of policy-making – and promoting understanding of the DPA 1998 in the workplace - both employee organisations interviewed stated a preference for collective agreements with employers. The TUC stated that UNISON[36] and the MSF were "advanced" on this issue[37]. Even where there was no trade union recognition, organisations should still be under an obligation to consult their workforces. This obligation will become compulsory for organisations employing 50 or more staff under the Information and Consultation Directive 02/14/EC, enacted in March 2002[38]. For the MSF, workplace agreements built on the legal provisions, adapting the legislation to specific circumstances of individual organisations. In this, the union had made progress. Generic model guidelines had been developed focusing on access to and monitoring of emails and internet use. The two key documents were a *Model Electronic Facilities Agreement* and a *Draft Code of Practice on Protection of Privacy at Work*[39]. Drafted in 1999, the interviewee believed: "the principles and the wording have stood up remarkably well to negotiations, challenges and so forth". When drafting the guidelines, reference was made to the International Labour Organisation (ILO) code of practice on the protection of privacy, some of the original research behind the OIC's *Draft Code of Practice: The use of personal data in employer/employee relationships*, and the ideas of a Union Network International IT working group which the interviewee chaired.

The core principles of both had been adopted in workplace situations, with allowances made for the particular circumstances of specific environments. For example, members based in customer-facing areas may favour the use of CCTV

for safety and security purpose, whilst those working in, for example, a postal sorting office may oppose the use of such cameras. Agreements have been signed with various government agencies and "some smaller businesses as well, although they are not yet at the stage of developing these things by and large"[40].

However, employers were more reluctant. Although UNICE recognised that some consultation with employees "is guaranteed by legislation", interviewees at the CBI believed it was up to individual organisations to draw up policies concerning employee data protection:

> "I think they would, as a general rule, be drawing up their policy themselves and not with the trade unions: it being the translation of legal obligations, not amendments to terms and conditions."[41]

The issue of policies for protection of employee personal data is considered in further detail in Chapter 7.

### 6.1.3 Transfer of personal data to third countries

Other general data protection issues that concerned interviewees included the transfer of personal data outside the European Economic Area (EEA), in particular to the US. This built on the context to this issue outlined in Chapter 4 (section 4.7). The 'Safe Harbor' agreement was described by the European Commission official as a "political success"[42] in that it allowed the EU and US to talk about data protection, something they had not done before. However, from a practical point of view, the results had been "scarce". At the time of interviewing (September 2001) only 100 companies had signed up to the agreement, and their compliance "appeared not to be good enough"[43]. This view was later supported in a European Commission working paper published in February 2002[44], also discussed in Chapter 4 (section 4.7.1).

Although the Commission was sceptical, UNICE supported the 'Safe Harbor' principles as a means of allowing businesses continuity in transborder flows of

personal data. Model contract clauses were viewed by the EU and business as a viable alternative, with applicability going beyond the US to all third countries. Approved by the European Commission in July 2001, the reception by business representatives was mixed. The CBI argued that it was impractical for organisations to draw up separate contracts for each of its global subsidiaries. The CBI interviewees preferred a single policy complying with basic international data protection rules, although they acknowledged:

> "...a fundamental difference in vision between Europe and the US over what is actually data protection."[45]

UNICE expressed concern that certain clauses concerning joint and several liability went beyond the protection outlined in Directive 95/46/EC. Their main fear was that the Commission's contracts would act as a benchmark, and disqualify other contractual clauses for the transfer of personal data to third countries. When the European Commission clarified this was not the case, a number of business organisations – including the CBI and American Chambers of Commerce – drafted alternative model clauses. To quote UNICE, the alternative models are: "intended to provide just as high a level of data protection as the Commission's clause, but using more flexible mechanisms that reflect business realities"[46]. Key differences between the EU and alternative model contracts included:

- Obligations on the exporter and importer of personal data revised to exclude obligations which go beyond the Directive. For example, clauses stating that exporter must explicitly inform data subjects that their data will be transferred to a country without an 'adequate level of protection' (Commission clause 4.b), and that a copy of the clauses must always be given to the data subject upon request (Commission clause 4.c), have been removed;
- Liability reflects existing data protection law (i.e., each party is liable for damages it caused), no joint and several liability;

- Selection of law governing processing by data importer is more flexible, and would allow a company to select a single set of principles (such as Safe Harbor) to cover its worldwide processing;
- Explicitly allows further transfers and multiple transfers to be covered.

The current position at January 2003 is that the European Commission introduced its model contracts, which member states' data protection authorities are obliged to recognise – in December 2001 (refer to Chapter 4). No decision has been made regarding businesses' alternative model.

### 6.1.4 Policy: data protection in organisations

During the case study interviews, the interviewees were asked about the key data protection issues impacting on their workplace. At expert interview level, Grant lucidly summed up the issues involving public organisations in her experience as a legal consultant to such bodies:

- Subject access requests (SARs). Organisations often did not have the technology to gather information from a large number of areas. This is especially true regarding personal data in emails;
- Transfer of data outside the EEA, a problem cited by employers organisations;
- Information systems. Not all data protection issues were considered prior to procurement of such systems: "It's after the contract's been awarded and the systems are actually been slowly developed, that those sort of issues would come up and have to be dealt with."[47]

In terms of overall written policy, Bird and Bird tended not to advise public organisations. In Grant's experience, they appeared to be more pro-active than the private sector, and have an appointed DPO. However, it was noted that the postholder tended to be at a low level in the authority, and usually did not ask for legal advice:

> "So, when I see data protection issues it's usually not because someone's come to me from a local authority to answer the questions, but I've raised an issue initially in procurement: "What are you doing about this? Have you taken some advice on this?" So, I think there is a level of compliance within authorities but it's not really a very high level."[48]

In summary, data protection generally – personal data belonging to both employees and clients - required a higher profile in public organisations. It lacked visibility and was perceived as an obstacle to progress rather than a service to an organisation in terms of systems development and records management. The status and role of the DPO in an authority was a topic which repeatedly came to the fore during case study interviews. Organisations were at a variety of stages. The key challenge perceived by Grant included the issue of data sharing and 'joined-up' government[49]: how and whether it is going to work. This partly overlapped with the work conducted by the Office of the e-Envoy (Oe-E), whose efforts in promoting electronic government are considered in the next subsection.

*E-government*

Policy concerning general data protection in public organisations forms a key part of the work of the Oe-E. Part of the Cabinet Office, the Oe-E was established in September 1999 with the aim of promoting access to, and use of, online facilities in the UK 'to ensure that the country, its citizens and its businesses derive maximum benefit from the knowledge economy'[50]. The key issues referred to at interview were data sharing and 'joined-up' government. In order to achieve these aims, part of the focus has been on increasing public trust in electronic service transactions, and specifically the question of the extent to which privacy could be protected. The end product of this was the draft *e-Trust Charter*, published in September 2001[51]. This represented government policy in this area, recognising the importance of data protection legislation in safeguarding privacy of personal data, whilst attempting to integrate public services. The *Charter* was perceived by the Oe-E interviewee as its key future challenge in "ensuring the design and delivery of electronic services"[52].

The *Charter* was to be displayed on all sites where the government delivered electronic services, seeking to reassure users of electronic public services about how their personal data will be handled. It envisaged that providers of electronic services would then offer context-specific privacy statements whenever personal information is requested from the public, covering each of the points in the *Charter*[53]:

- Who will see the personal data;
- Why they need it;
- What they will do with it;
- When they will deleted.

Additionally, public organisations are expected to inform individuals:

- How they will safeguard their personal data;
- How individuals can check and correct their personal data;
- How to pursue a query or complaint;
- Where to get more information.

The Oe-E perceived the *Charter* to be relevant for both government departments and the wider public sector, proving a useful policy tool for achieving data protection compliance in the electronic environment. In April 2002, the draft *Charter* was subsumed within the 'Public Services Trust Charter' as detailed in the Performance and Innovation Unit's report on *Privacy and data-sharing* published that month[54]. The significance of this report is referred to throughout this thesis.

*Safeguarding personal data online*

In January 2001, Consumers' International (CI) produced similar recommendations for all organisations in its report *Privacy@net*[55] discussed in the Literature Review (Chapter 3, 3.1.5). CI had worked with the US civil liberties group and research centre, EPIC, to write the report and recommendations. CI's research showed that the majority of websites surveyed ignored basic principles of

information use that had underpinned data protection legislation for the last three decades. These included: giving consumers control over the collection and use of their information; giving them a right to access and collect that information; and ensuring security of their data. A practical tip sheet was enclosed for consumers who wanted to protect their privacy online[56].

Released nine months prior to the draft *e-Trust Charter*, the report recommended that all sites that collect information from users should provide a privacy policy that clearly stated their policy towards individual's personal data. The policy should be signposted clearly from the home page, and at every point within the site where personal information is collected. The privacy policy should include:

- The identity of the company that owns and operates the site;
- The kind of information collected;
- Why the data is stored and what it is used for;
- Who the data is shared with (including a list of affiliates), and what choices the user has about this;
- How long the data is stored for;
- How the security of that data is ensured;
- How consumers can access, alter and delete their data;
- How the site's policy might change in the future;
- Contact details for the person responsible for the privacy of data;
- Contact information for the pertinent oversight body.

The privacy policy was similar to the draft *Charter*. In some respects it went further, with the provisions concerning who the data is shared with and how the site's policy may change - attempting to counter commercial realities of mergers, takeovers and the sale of personal data to third parties. The report called for establishment of an independent oversight body to 'ensure compliance and provide for adequate sanctions for violations'[57]. At interview, it was stated that this body should be either European or global, comprising lawyers and IT experts. As the interviewee stated: "You can't ask us to accept that US businesses set the standards"[58].

### 6.1.5 Human Rights Act 1998

The HRA 1998 was referred to in many interviews. Interviewees saw its advantage in bolstering the provisions of the DPA 1998. The most detailed observations on the HRA 1998 were gained through interviews with JUSTICE, the JCHR, and Grant. JUSTICE appraised the Act as a "very politically astute document" that was balanced – incorporating the concerns of the media concerning freedom of expression – and clear and workable[59]. However, JUSTICE were keen to stress that the HRA 1998 lacked the weight of a constitutional Bill of Rights, and there was no guarantee that the individual's constitutional rights would always be protected. Finally, there was a lack of training in public authorities, other than central government. JUSTICE had worked with the Local Government Association in an attempt to remedy this.

Feldman, the legal policy advisor to the JCHR, was "very impressed" with cooperation from government departments – particularly the Home Office over the anti-terrorism measures that were being discussed at the time of interview (November 2001). More broadly, Feldman believed a common law had been developed in the wake of the 2000 *Douglas* case, involving the taking and planned publication of illicit photographs at the wedding of actors Michael Douglas and Catherine Zeta Jones:

> "I don't think that there's very much doubt that there's a right of common law privacy. Who's to say how far it's been influenced by the Article 8 point. I think that having certain obligations under Article 8 does no harm at all."[60]

Overall, the transition to HRA 1998 had been smooth. Certainly, in Feldman's view, the judiciary had been well-trained and central government departments been very effective prepared. In the interviewee's experience, there had been no lack of awareness, although, unsurprisingly, some lack of understanding on the more technical legal issues.

At Bird and Bird, the perspective of Grant was that the HRA 1998 was "bedding itself down" and the higher courts had been conservative in their interpretations regarding privacy[61]. Horizontal effect – that is, the HRA 1998 being applied outside of public authorities – was certainly evident with courts and tribunals interpreting certain cases. This was a view supported by Feldman and JUSTICE. An example given by Grant was that of Leonard Cheshire Homes[62], stating that local authorities, even when contracting out work, still had to ensure the organisations that were working for them complied with the HRA 1998. The HRA 1998 appeared to be clear and workable. Awareness of the Act was high in public organisations, although there was uncertainty as to what it meant in practice. These observations were borne out during the case study interviews.

### 6.1.6 Freedom of Information Act 2000

More practical awareness was to be found concerning the implications of FOIA 2000 – something strongly supported during the case study interviews. Interviewees at the Lord Chancellor's Department perceived this legislation as its "key challenge"[63]. The supervisory model enacted by the UK government of one Information Commissioner balancing both FOI and data protection was perceived as more consensual than having two Commissioners each championing their own causes[64]. It was observed that the OIC already had a strong role in promoting and enforcing openness of information. The key tests were perceived by the Lord Chancellor's Department to be:

- Implementation of FOIA 2000 – and how it would impact on the extended scope of the DPA 1998;
- The reaction of the courts to FOIA 2000. Whilst the DPA 1998 was underpinned by international law, the case for FOIA 2000 was less certain[65];
- The need for sound information handling practices. Can public organisations find information requested under FOIA 2000?

The leading campaigner for freedom of information, the CFOI, had developed good contacts with the Lord Chancellor's Department, with a member of staff seconded to the Department at the time of interview (November 2001). Like the Lord Chancellor's Department, the CFOI perceived difficulties with data protection being given precedence over FOI due to its European roots. The effect of the HRA 1998 on FOIA 2000 was viewed by the CFOI as "indirect":

> "I think the FOI Act is explicit enough in most cases, it doesn't leave too many opportunities or areas where it would have an impact."[66]

However, the greatest difficulty the CFOI experienced with FOIA 2000 was that "the government doesn't want to implement it", having just announced at the time of interview that the implementation of the provisions were to be delayed until January 2005. Additional problems cited included rights of access were very weak, with many depending solely on the balance of public interest test, where ministers have the right of veto. Moreover, other exemptions were "much too broad"[67]. These exemptions, including 'information provided in confidence', and 'prohibitions on disclosure by enactment' were discussed in Chapter 5 (section 5.4.3).

Like JUSTICE, CFOI had provided a training service in its field of expertise. A general guide to the individual's right to information had been produced and training had been organisated for public authorities – either directly, or through speaking at conferences. At the time of interview, the workload was decreasing with the non-implementation of the Act. However, demand was expected to rise when implementation becomes imminent.

### 6.1.7 Anti-terrorism

Anti-terrorism concerns were thrust into prominence following the attacks of 11th September 2001. As one legal advisor to the government stated: "Terrorism is now a priority. Within this, data protection is of key importance."[68] During the period of the interviews, the UK government considered various initiatives

including issuing of national identification cards, derogating from Article 5 – right to liberty and security of person - of the ECHR, and retaining communications data. These initiatives will be considered in turn. Many of the government's proposals came together in the ATCSA 2001, enacted in December 2001 and discussed in Chapter 5 (section 5.5). All but one of the expert interviews took place prior to the passing of this Act. Yet, various concerns were voiced by interviewees.

The interviewee at the OIC stated that any national ID system would be "flawed from the start", as the government would have to compile a database covering the identities of the national population[69]. The issue of which system to base this database on would cause major difficulties. One of the largest databases in the UK – concerning National Insurance (NI) numbers – contains more NI numbers than there are residents in the UK[70]: "If you use that system which is inaccurate as a basis for any new system, it is automatically flawed."[71] Additionally, identity cards have existed in Spain for almost 60 years[72], and yet internal terrorist movements are still successful. In July 2002, the UK government confirmed that it favoured the introduction of national 'entitlement cards', and launched a six-month consultation period into the issue[73]. The consultation document stated that the government 'would ensure the scheme fully complied with the Data Protection Act 1998'[74].

Concerning the derogation from Article 5, Feldman explained it related only to immigrants who posed a threat to national security and could not be deported because there was nowhere safe to deport them to, as deportation would violate their Article 2 (right to life) or 3 (prohibition of torture) rights. In those cases only, the UK government are "going to take a power to detain those people in this country rather than throw them out in violation with their other more important rights"[75]. Feldman did not believe the UK government disregarded human rights at all, and thought it was "unfortunate that that impression is created"[76].

Regarding data retention, the CBI raised fears at interview in November 2001 – a month prior to the enactment of the ATCSA 2001. The Act's voluntary code allowing for data retention had yet to be drafted[77], but there was unease as to how

it would interface with RIPA 2000, which allows access through the issue of warrant or authorisation. The assumption is that there is going to be an increase in the amount of data that companies – such as (internet service providers) ISPs - are expected to retain and then disclose to law enforcement agencies. Naturally, this will result in issues of trust in how the retention will be presented to business clients, in addition to cost implications in terms of storing and accessing the data:

> **"I think businesses are probably aligned very much against it because they're aware of the cost implications."[78]**

## 6.1.8 Conclusions

The expert interviews have provided an overview, a useful snapshot of opinion on a number of issues ranging from the text of the DPA 1998 to broader human rights concerns and the establishment of a privacy common law. Moreover, the events of 11 September 2001 – and heightened interest in acquiring personal data as a result - demonstrated how relevant data protection concerns are now. Although the UK government has stated its anti-terrorism measures comply with the requirements of both the DPA 1998 and the HRA 1998, many of the interviewees were uneasy. The interviews raised the following key issues, some of which complement findings from previous Chapters:

(i) *Need for legal clarity.*

The interviewees heavily criticised the wording of the DPA 1998, describing it as "appallingly drafted" and "ambiguous". A practising lawyer stated that clients found the text "convoluted" and were overwhelmed by guidance surrounding terms such as 'structured filing system'. Moreover, there were clear problems concerning important terms such as 'consent', which lacked any definition in the Act[79]. The task of OIC in providing the necessary detailed guidance appeared particularly onerous. The text of the DPA 1998 is undoubtedly complex, comprising 75 sections and 16 schedules. Moreover, 19 separate sets of secondary

legislation[80] have been produced by central government – adding greater depth to, and frequently clarifying - the provisions of the 1998 Act.

(ii) *Reconciling data protection with e-government.*

The interview with the Oe-E highlighted the tension between the government's obligations under the DPA 1998 and HRA 1998, and their drive to coordinate and integrate public services. At the time of interview (October 2001), the Oe-E was promoting the *e-Trust Charter* – later the 'Public Services Trust Charter' - to reassure the public about their personal data when using online public services. Case study interviews in public authorities in Chapter 7 expound on this issue, with many local authorities being assessed on their "e-government agendas", rather than compliance with the DPA 1998.

(iii) *Specific difficulties presented by employee personal data*

The EU and the OIC appeared to have difficulty getting to grips with the specific issue of employee personal data. The sensitivity of the information involved, the fact that it could be accessed – and abused – by colleagues of the employees, and the unequal relationship between employee and employer were among the factors convincing interviewees within the EU, OIC and trade unions that further action was necessary.

To this end, the interviewee at the European Commission had drafted a working paper on the issues with a view to legislating in the near future. However, UNICE did not see the need for further regulation, preferring instruments such as codes of practice, voluntary instruments and guidelines[81]. The OIC – who had worked closely with the EU interviewee on the working paper – were experiencing difficulty in pitching their *Employment Practices Data Protection Code* to the appropriate audience. The CBI viewed the OIC's *Code* – half of which is still in draft form - as interfering with business working practices, and failing to take into account the daily administrative needs of small businesses in particular. However, at a local, bottom-up level, real progress appeared to be being made, with the MSF entering into collective agreements with various organisations. The reason for the

union's success perhaps hinged on the codes being flexible enough of meet the individual needs of organisations, rather than being blanket regulations imposed from above.

(iv) *Interface between the provisions of the DPA 1998, and other legislation.*

Supporting the findings of Chapter 5, the key legislation referred to by interviewees were FOIA 2000, HRA 1998 and the proposed anti-terrorism measures. FOIA 2000 was recognised as having a huge impact on the data-handling practices of public organisations, being perceived by the Lord Chancellor's Department as its "key challenge". Implementation of the Act, its impact on the extended scope of the DPA 1998, and the reaction of the courts to the new Act were all perceived by the government to be important tests. Understanding of the practicalities involved in the HRA 1998 and anti-terrorism legislation for organisations was less clear. For the HRA 1998, this was due to the general nature of its provisions and small, but growing, amount of case law concerning the legislation. The anti-terrorism measures were under discussion at time of interviewing, thus the interviewees were unable to comment on their possible impact.

The above issues have significant consequences for public organisations seeking compliance with the provisions of the DPA 1998. The questionnaire survey analyses views from practitioners.

## 6.2 Questionnaire survey

This survey measured practitioner awareness and informed opinion concerning the DPA 1998. In particular, the survey sought to assess the challenges facing organisations regarding the handling the employee personal data. Additionally, data protection issues surrounding relevant legislation such as FOIA 2000, HRA 1998 and RIPA 2000 were considered. The aim of the survey was not to achieve statistical significance, which would have been difficult to justify in a PhD study

concerned with measuring organisational policy and best practice. Instead, the aim was to yield indicative data that could be triangulated with findings from expert interviews. Indeed, an important justification for conducting this survey was to develop contacts for case study interviews. In this respect, the survey was very successful, with 18 respondents ultimately participating in the case studies.

The questionnaire survey was initially piloted on eleven organisations in February 2001. The questions were devised following desk research into the legal context behind UK data protection legislation. Following feedback, amendments were made to the questionnaire format. In September 2001, 382 questionnaires were distributed to a variety of public organisations including local authorities, health authorities, universities and police authorities. The final number of replies was 107, representing a response rate of 28.0%. Table 5 below breaks down the respondents by organisational type.

| Type of organisation | Number of questionnaires received |
|---|---|
| Local authorities | 89 |
| Universities | 9 |
| Health authorities | 3 |
| Police authorities | 1 |
| Quangos | 2 |
| Privatised utilities | 3 |
| | |
| Total | 107 |

Table 6: Questionnaires received by category

This section examines findings from a selection of questions posed during the survey. Questions were chosen for analysis based on the relevance and usefulness of the data in relation to the overall aim, hypotheses and objectives of this thesis. A copy of the full questionnaire survey is included in Appendix D. The data contained in the bar charts and pie charts in this section have been described using actual numbers, as an over-reliance on percentages would have been misleading.

Where data concerning the responses has been given in the text, two numbers are displayed in brackets – for example (33, 30.8%). The first number relates to the actual number of responses; the second to the percentage of the total that this represents. Percentages are given to one decimal place. The data displayed is illustrative only – providing a 'snapshot' of public authority opinion and awareness concerning the DPA 1998 and related issues.

In this section, each question posed is presented in bold, followed by a brief analysis of the responses. For ease of reference, the numbering of the questions corresponds with their numbering in the full survey. The following abbreviations are used: 'DK' for 'don't know' and 'DNA' for 'did not answer'.

### 6.2.1 Data analysis

**1. Does your organisation have a nominated member of staff with responsibility for data protection?**

| | | **Percentage (%)** |
|---|---|---|
| **Yes** | 103 | 96.2 |
| **No** | 2 | 1.9 |
| **D/k** | 2 | 1.9 |
| Total | 107 | 100.0 |

Table 7: Respondents with nominated staff responsible for data protection.

Almost all respondents stated that they had a nominated member of staff responsible for data protection in their organisation. Only two (1.9%) explicitly stated that they did not, and both were in the process of creating a position. This demonstrated, at the very least, that the respondents had acknowledged the existence of UK data protection legislation.

## 2. What steps has your organisation taken to comply with the DPA 1998?

The results from this question are displayed in Figure 2 overleaf. The most popular steps taken to achieve compliance with the DPA 1998 were internal audit (85, 79.4%) and in-house staff training (85, 79.4%). The latter was confirmed during the case study interviews, where almost all interviewees stated that data protection training was conducted by the organisational Data Protection Officer (DPO). Less than one third (33, 30.8%) of organisations had used external trainers – a finding that again was borne out at interview, and ascribed to the expense involved in hiring outside organisations. One case study organisation had received quotes of £5 000 - £8 000 to receive a day's training for up to 25 people. So, where possible, training was conducted in-house.

**Measures taken to comply with DPA 1998**

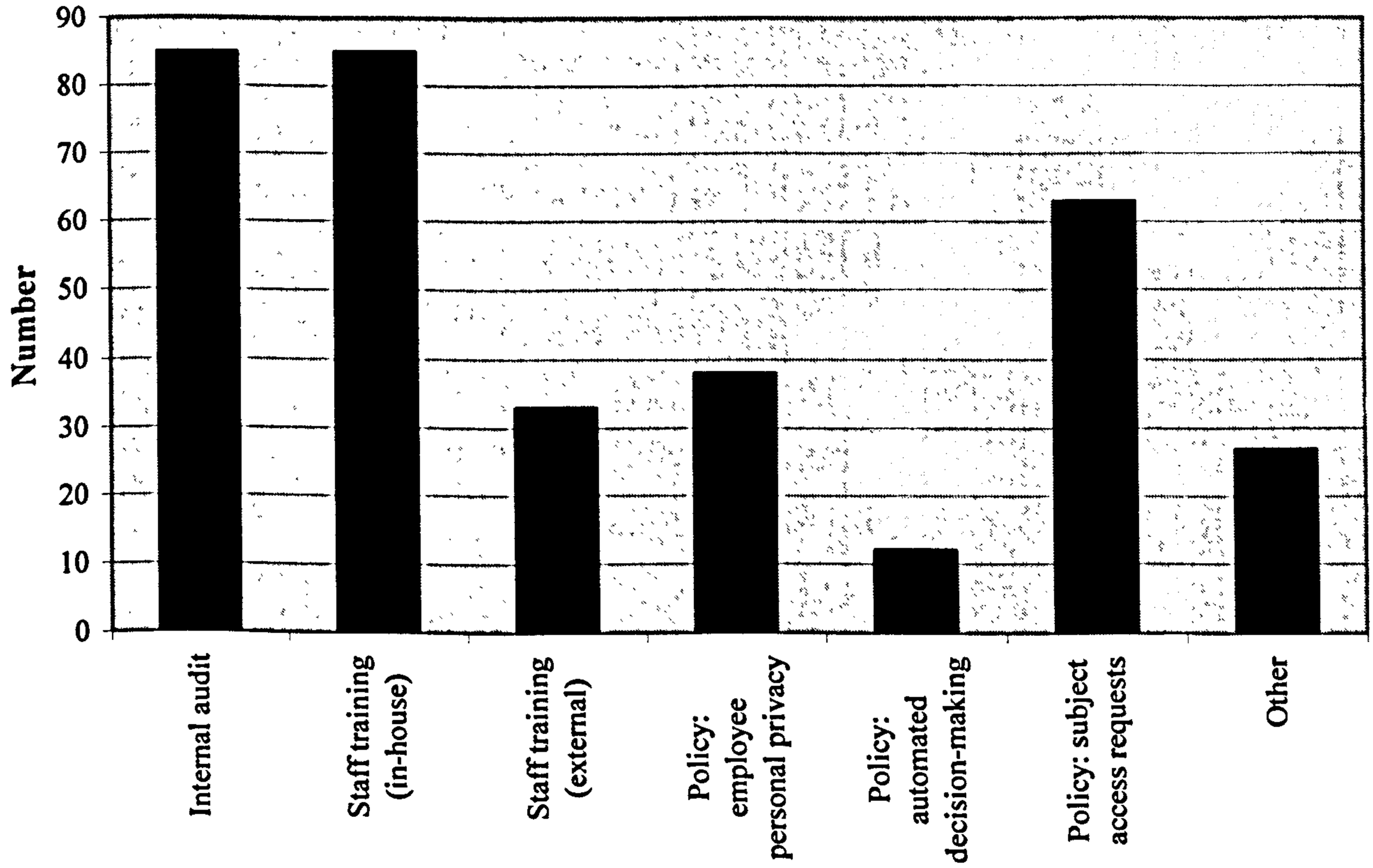


Figure 2: Measures taken to comply with the Data Protection Act 1998

In terms of policy-making, the questionnaire aimed to assess the *presence* of policies in organisations, rather than their actual contents. However, a small number of respondents did mail copies of actual documents. These documents

tended to be general statements informing the public of their rights to information under the DPA 1998, with advice on exercising this right. Organisational policies are discussed in detail in Chapter 7 (section 7.6). Over half the survey respondents (63, 58.9%) had devised policies for handling subject access requests – a key element of the DPA 1998. A little over a third (38, 35.5%) had a policy concerning employee personal privacy and 12 respondents (11.2%) had a policy concerning automated decision-making. Case study interviews established that most organisations were still in a state of flux regarding this issue.

Other compliance measures were cited by 28 (26.2%) of respondents. They included:

- Amending application forms to inform applicants of the purposes their personal data will be put to;
- ICT security policies;
- Establishment of data protection working groups;
- Informing staff of developments through newsletters, email circulars and information printed on their payslips.

**7. What are the subject access procedures for employees asking to view their records?**

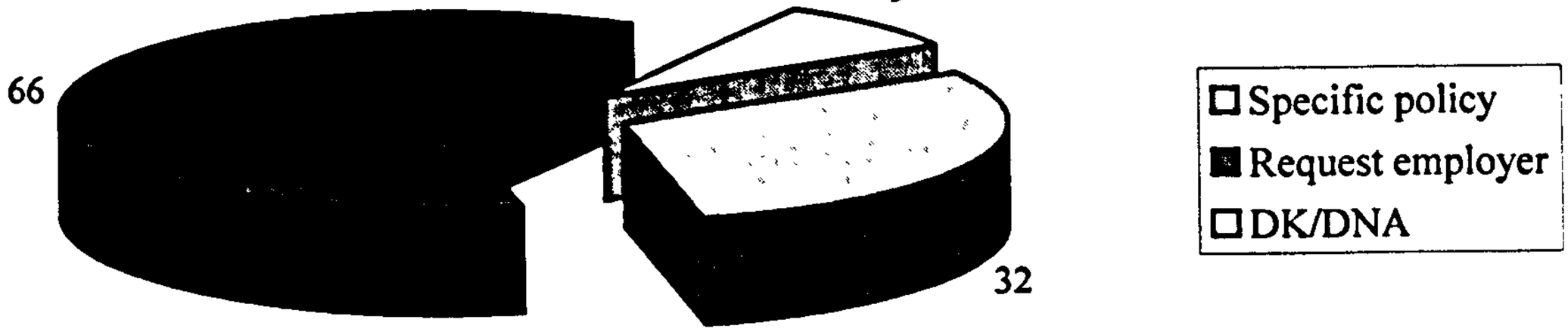


Figure 3: Provisions for employees requesting their own personal data.

The right of subject access request is a fundamental right under the DPA 1998, allowing the data subject to exercise other rights such as the rectification, blocking, erasure and destruction of inaccurate or incomplete personal data. Subject access procedures are discussed in further detail during the case study analysis (Chapter 7, section 7.5).

From the analysis of the questionnaire data, only 32 respondents (29.9%) had specific policies in place regarding employee access to their personal data. 66 respondents (61.7%) did not have a formal policy, but made personal data available on request. Finally, nine (8.4%) either did not answer the question, or did not know the situation regarding employee subject access requests. These findings contrasted with those of the case study interviews, where 15 out of the 18 organisations interviewed had developed well-defined subject access procedures.

## 8. What are the security procedures in place for safeguarding employee records?

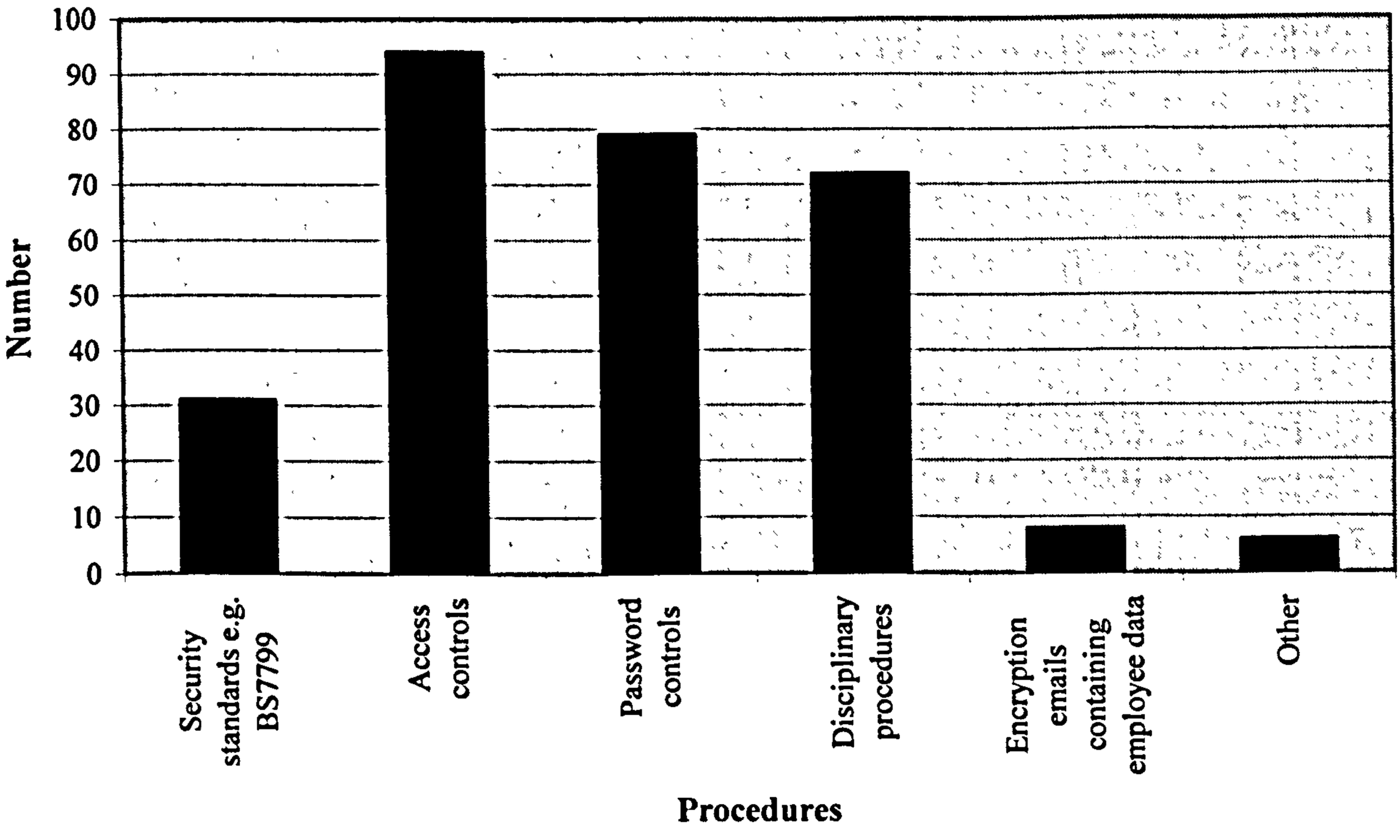


Figure 4: Procedures for safeguarding security of employee records.

Principle 7 of the DPA 1998 states that 'appropriate technical and organisational measures' must be taken to safeguard personal data. Nearly all respondents (94, 87.9%) had controls regarding access to employee personal data. A popular control was use of passwords to restrict access to certain types of record (79, 73.8%). Moreover, the majority of organisations (72, 67.3%) had formal disciplinary procedures in place to combat any breaches of data security.

Technical measures safeguarding security were less common. Less than one third (31, 29.0%) of respondents claimed compliance with formal security standards such as BS 7799 - the British Standard for *Information security management*[82]. One reason for this, supported during the case study interviews, was the time and expense involved in achieving compliance. Eight respondents (7.5%) encrypted emails containing employee personal data.

**9. Does your organisation have a formal policy concerning staff use of:**

**i. Email**

**ii. Internet?**

| | Yes | No | Total |
|---|---|---|---|
| **Email** | 100 | 7 | 107 |
| **Internet** | 100 | 7 | 107 |

Table 8: Policy concerning staff email and internet usage.

The need for a detailed policy governing employee usage of email and the internet has been the subject of much media debate since the OIC released its *Draft Code of Practice* in October 2000[83]. It is telling that at the time of writing (January 2003), over two years following the publication on the draft *Code*, the section concerning *Monitoring at work* has yet to be finalised. The latest version of the section recommends employers draft a policy concerning monitoring of communications and communicate this to employees. This issue was discussed in interviews with both employer and employee representatives (section 6.1.2).

The overwhelming majority of respondents (100, 93.5%) claimed to have such policies – all combined policies - concerning staff usage of email and the internet. However, this was not borne out during the case study interviews, where only half had actually devised such policies. The complexities of policy-making in this field are discussed in Chapter 7 (section 6).

**10. Does your organisation monitor staff use of:**

i. **Email;**

ii. **Internet?**

| | Yes | No | Total |
|---|---|---|---|
| **Email** | 79 | 28 | 107 |
| **Internet** | 88 | 19 | 107 |

Table 9: Respondents monitoring staff email and internet usage.

Perhaps in response to media reports of employee abuse of email and internet usage – and the resulting fear of legal action - levels of monitoring were very high. 79 respondents (73.8%) monitored staff email use. A higher number (88, 82.2%) kept track of internet usage, perhaps due to the ease at which pornography could be accessed online.

***Questions 11 and 12 were aimed at respondents who answered 'yes' to either or both 10 (i) and 10 (ii).***

**11. How frequently does your organisation monitor use of email and/or the internet?**

The data for this question is presented in Figure 5 overleaf. In all, 90 respondents answered this question. Almost half of those who monitored employee use of email and internet did so 'only with good reason' (41, 45.6%). The next most popular answer was daily (25, 27.8%). However, a total of only 27 respondents (30.0%) monitored more than once a month.

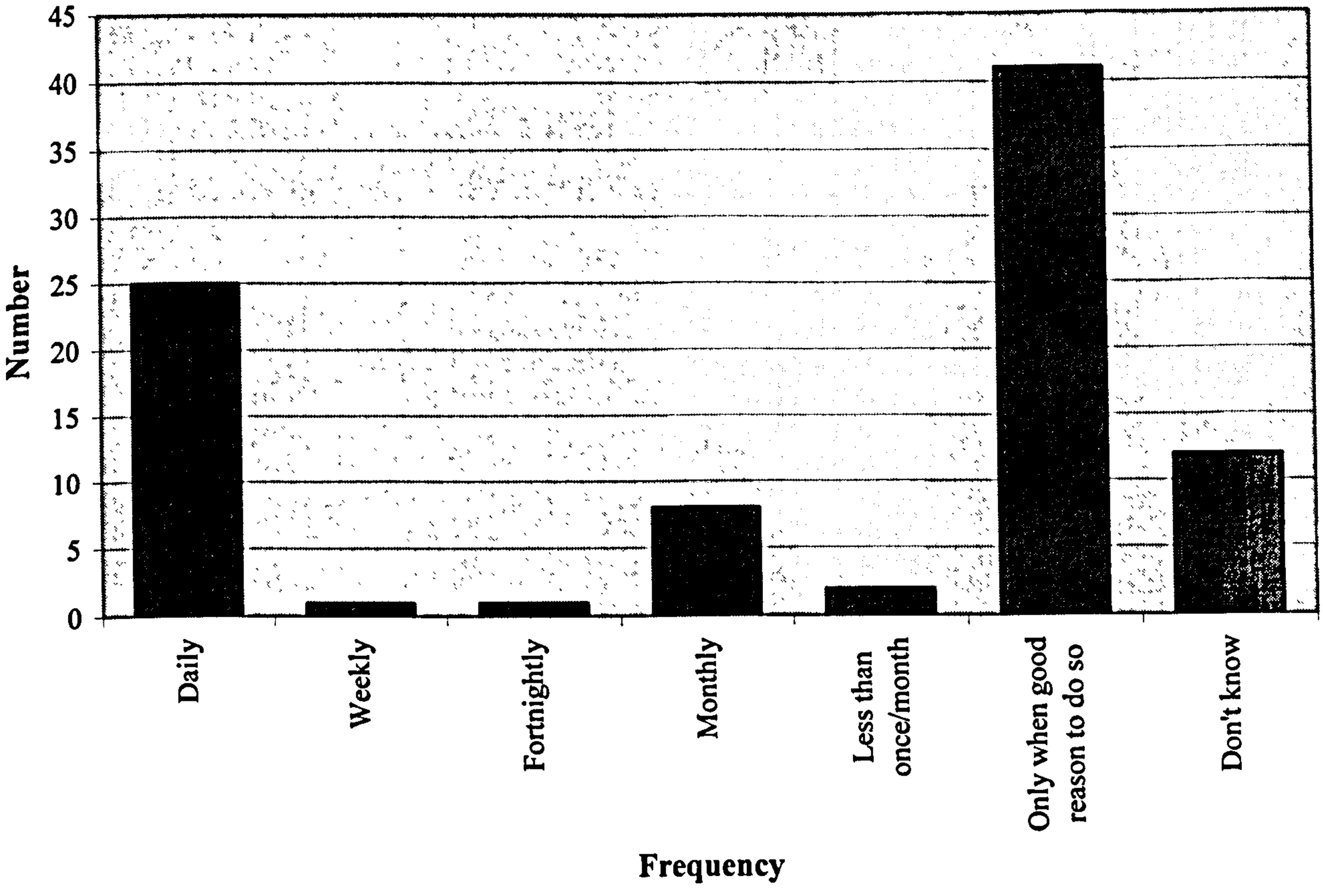


Figure 5: Frequency of monitoring of staff email and internet usage.

This is in line with guidance on this issue in the OIC's latest version of part three of *Employment Practices Data Protection Code – Monitoring at Work.* Under the section of the draft *Code* entitled 'Monitoring communications', the OIC advises organisations to:

> 'Make an impact assessment to determine what, if any, monitoring of electronic communications is justified by the benefits. Limit the scope of monitoring to what is strictly required to deliver those benefits.'[84]

The Code proceeds to state that established methods of supervision should be considered prior to any monitoring.

## 12. Is email/internet use monitored automatically?

Over half the 90 respondents (49, 54.4%) stated that they monitored email and/or internet usage automatically. Software products mentioned included: *1-gear*; *Mailsweeper*; *Surfcontrol*; and *Webtrends*. Less than a third of respondents (28, 31.1%) did not automatically monitor email and/or internet usage.

**Automatic monitoring of email and internet usage**

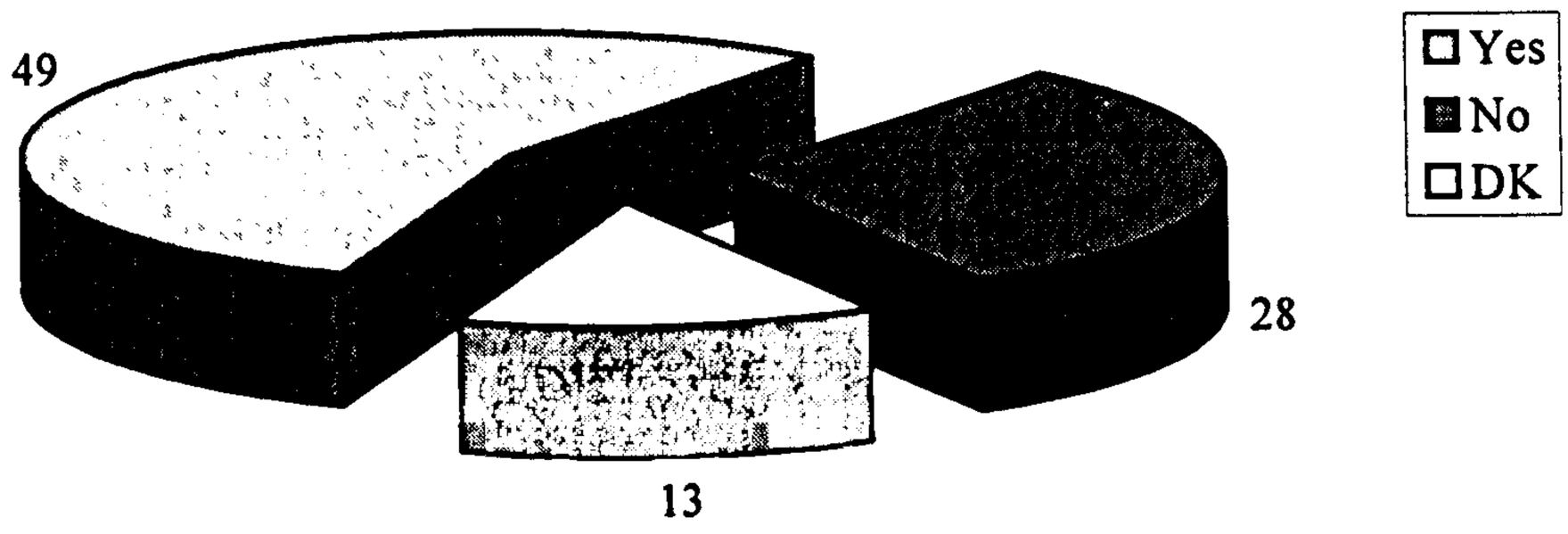


Figure 6: Respondents monitoring staff email and internet usage automatically.

## 13. Is your organisation aware of:

- ***Draft Code of Practice on the use of personal data in employer/employee relationships*;**
- ***Lawful Business Practice Regulations* (*LBPR*) – part of RIPA 2000;**
- **HRA 1998?**

Figure 7 demonstrates that overall awareness was high – attributed to levels of training and the media coverage the above legislation and guidance have received. Nearly all respondents (104, 97.2%) were conscious of the HRA 1998, and the overwhelming majority mindful of the draft code of practice (98, 91.6%). Awareness concerning the LBPR was lower at 73 organisations (68.2%), but still impressive for a piece of secondary legislation.

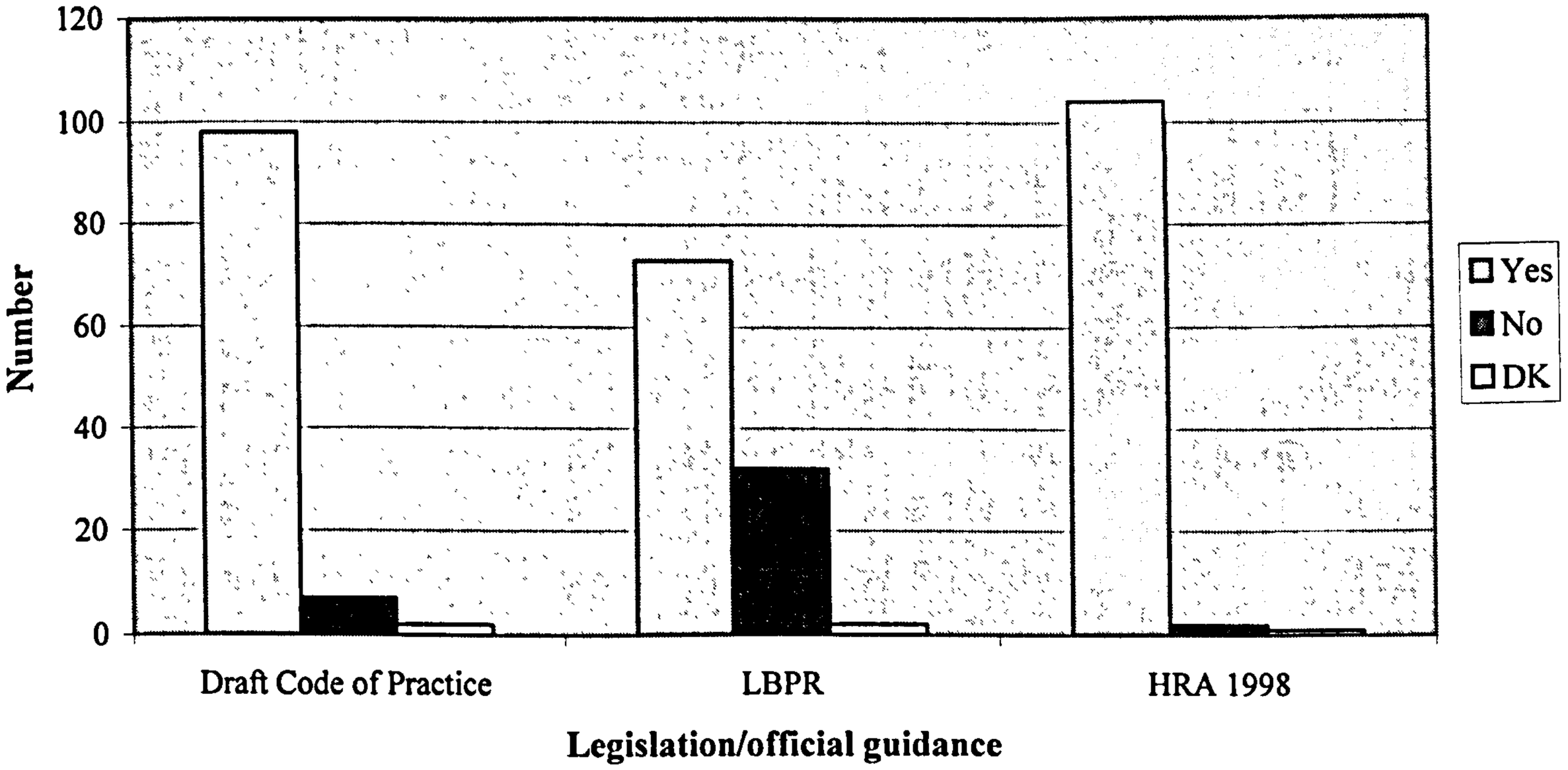


Figure 7: Respondent awareness of legislation and official guidance.

**14. Please indicate the degree to which you agree with the following statements:**

(i) **The *LBPR* represent a positive measure for ensuring compliance and good practice;**

(ii) **The DPA 1998 represents a positive measure for ensuring compliance and good practice;**

(iii) **The HRA 1998 will have a considerable impact on our organisation's handling of personal data;**

(iv) **Official guidance concerning the DPA 1998 has been clear and practical;**

(v) **Official guidance concerning the HRA 1998 has been clear and practical.**

- Figure 8 overleaf shows results for **14 (i) and (ii):**

**The *LBPR* and DPA 1998 represent positive measures for ensuring compliance and good practice**

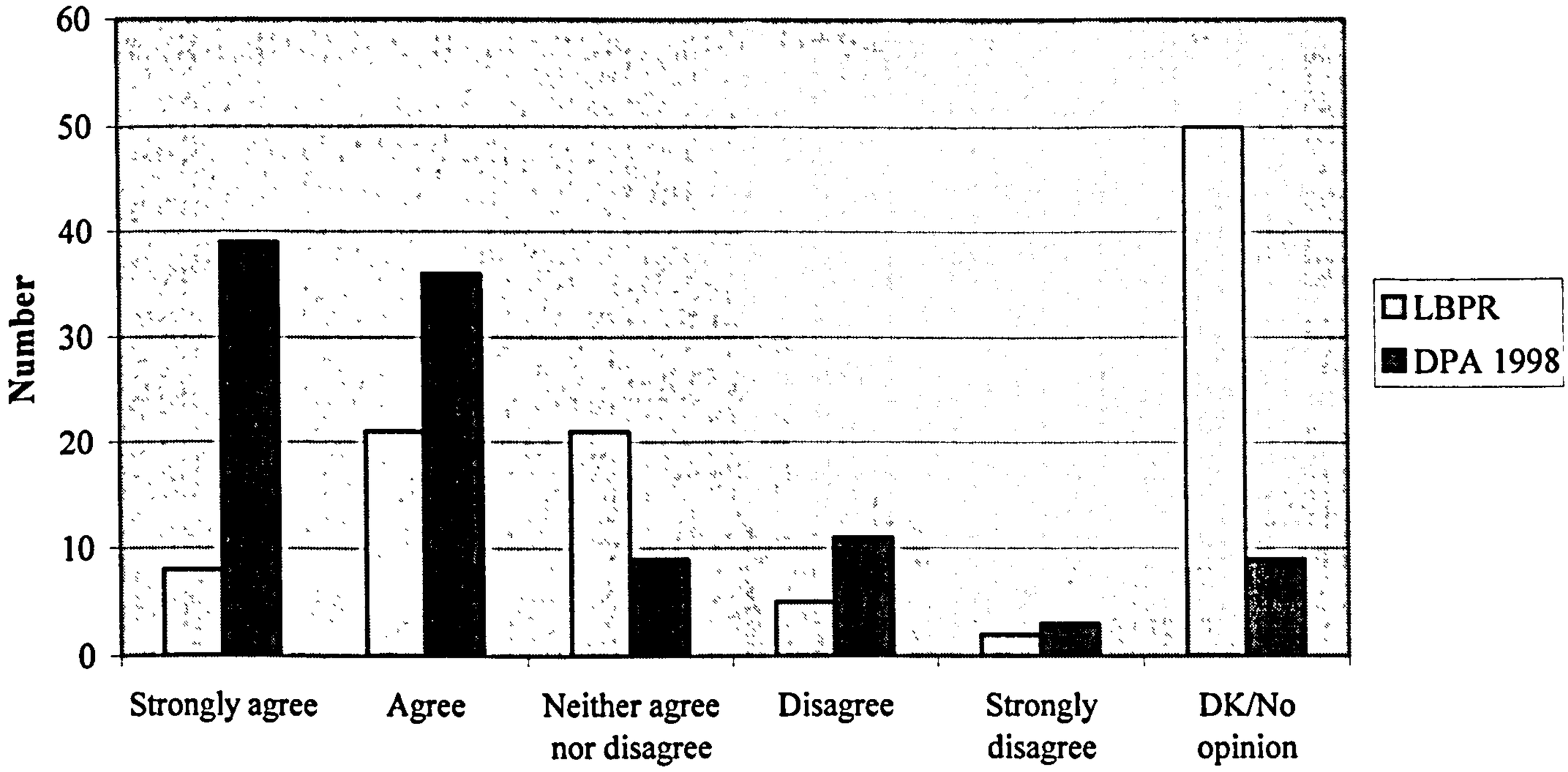


Figure 8: Respondent views on the *Lawful Business Practice Regulations* and the Data Protection Act 1998.

Opinion on the *LBPR* was unclear, perhaps reflecting the lower level of awareness (refer question 13). The most popular response was 'don't know/no opinion' (50, 46.7%), with a further 21 respondents (19.6%) neither agreeing nor disagreeing with the statement. Thus two thirds of respondents has no clear opinion concerning the *LBPR*. However, only 7 respondents (6.5%) disagreed or strongly disagreed with the statement that the *LBPR* are a positive measure. This is in spite of some negative press coverage concerning this legislation, stating that the *LBPR* contributed to a confusing legal environment concerning monitoring of employee data[85].

Opinion concerning the impact of the DPA 1998, however, is more clear-cut. Most respondents strongly agreed or agreed (75, 70.1%) that the DPA 1998 is a positive measure for ensuring compliance and good practice. Only 14 respondents (13.1%) disagreed or strongly disagreed with this viewpoint. These findings were confirmed in the case study interviews. However, many case study organisations

– and expert interviewees – found the text of the Act 'convoluted' and generally poorly drafted. Thus, although practitioners generally agreed with the aim and intentions of the DPA 1998, there were problems with the drafting of the legislation and some of the official guidance – considered below.

Figure 9 shows the results for question **14 (iii)**:

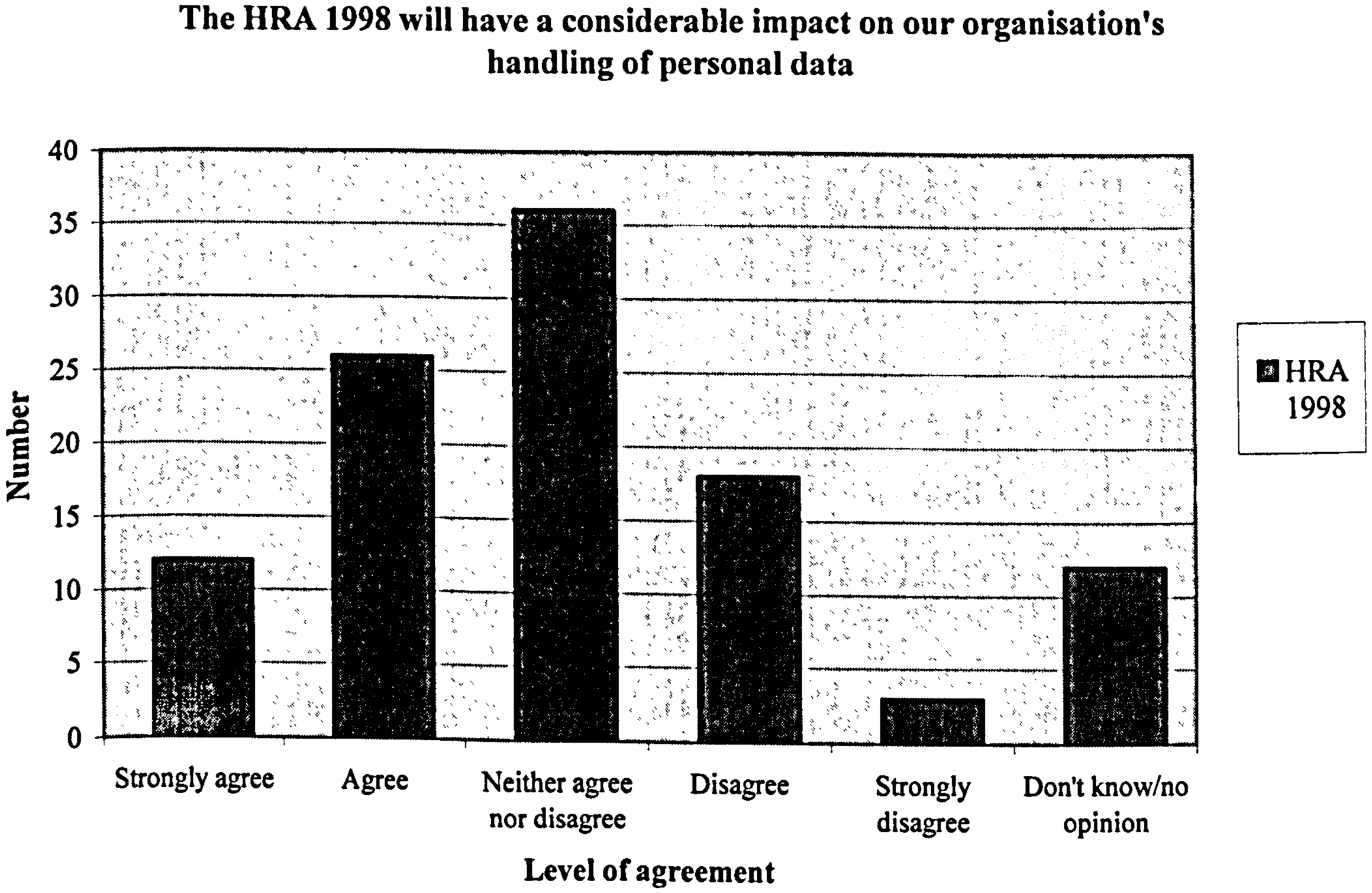


Figure 9: Respondent views concerning the impact of the Human Rights Act 1998.

Opinion concerning the impact of the HRA 1998 on organisational personal data handling was not particularly strong. The most popular response was 'neither agree nor disagree' (36, 33.6%), with an additional twelve (11.2%) stating 'don't know/no opinion'. Thus, more respondents (48, 44.9%) had no clear opinion concerning the impact of the Act, than any stated view. This could reflect a lack of guidance on the HRA 1998, or perhaps the feeling – gained during case study interviews – that the HRA 1998 only applies to organisations in a rather distant, indistinct, way. 38 (35.5%) respondents agreed or strongly agreed that the HRA

1998 would have a considerable impact, whilst 21 (19.6%) disagreed or strongly disagreed with the statement.

Figure 10 below shows the results for both questions **14 (iv)** and **(v)**. Opinion concerning official guidance on the DPA 1998 was generally positive. 46 respondents (43.0%) either agreed or strongly agreed that the official guidance has been clear and practical. However, a significant minority (28, 26.2%) disagreed or strongly disagreed with the statement. Case study interviewees revealed frustration in some quarters at varying interpretations given to issues surrounding this complex piece of legislation by official bodies such as the OIC.

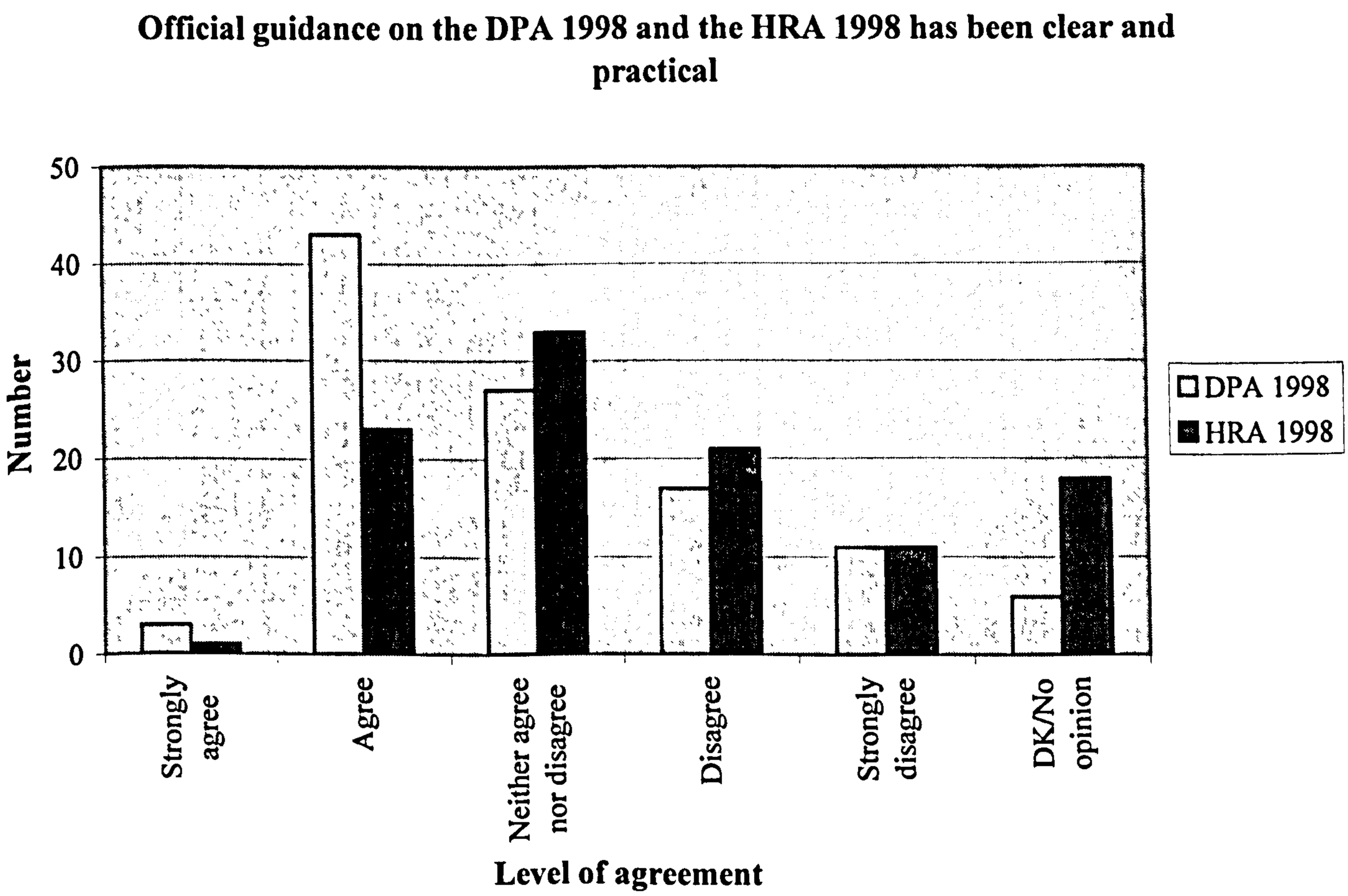


Figure 10: Respondent views concerning official guidance on the Data Protection Act 1998 and the Human Rights Act 1998.

Concerning the HRA 1998, the above chart demonstrates that responses were similar to those given in answer to question 14 (iii), reflecting the general vagueness – and perhaps lack of understanding – surrounding the statute. Again,

the most popular answer was 'neither agree nor disagree' (33, 30.8%). Where opinion was given concerning official guidance on the HRA 1998, it was more negative than positive. 32 respondents (29.9%) disagreed or strongly disagreed that the guidance had been clear and practical, whilst 24 respondents (22.4%) agreed or strongly agreed with the statement.

**15. Any further comments?**

Useful feedback was received concerning a wide range of issues brought up by the questionnaire. Most comments related to the DPA 1998, and official guidance by the OIC. However, there was input concerning records management, the likely impact of the HRA 1998 and whether employees were entitled to privacy in the workplace. For ease of reference, the following comments have been categorised by issues they relate to:

*Records management*

'As part of a wider organisation, we receive information from the relevant departments. We have been asked about records kept re public. Having received this questionnaire, I will certainly follow up the relevant legislation and familiarise myself. Thank you';

*DPA 1998 and official guidance*

'The move from implementation phase one to two of the DPA did not receive good advance publicity last month [October 2001] – much more should have been to alert/remind data controllers';

'The Act is very weak in that it does leave so much undefined, and therefore guidance needs to be stronger to fill the gap until case law becomes effective. To this end, there has been little or no government support and the Commissioner's information is very poor – the amateur website is an example.

'No-one has bothered to think it [the DPA 1998] through for its user, or the person who is data controller – and frankly the video is bigoted, sexist, portrays stereotypes and has little of use in the way of help';

'Areas of ambiguity exist in the draft Code relating to the DPA 1998. This is not helpful to employees responding to the legislation, or where deadlines are imposed';

'Official guidance [concerning the DPA 1998] not yet fully implemented/agreed. Would be nice to get firm decisions';

'The advice given by the Information Commission is good and practical. The problem is that the DPA itself is unclear and woolly'.

*Employee privacy in the workplace*

'We do not believe that staff have the right of free use of communications equipment that they do not own or pay for. All staff are made aware of the situation. For the same sort of reason we do not allow staff to use office addresses as personal 'mail' addresses. Many staff use mobile (personal) phones for 'private' matters';

'I have strong views on privacy and human rights in the workplace, and I am opposed to bosses snooping on their workers'.

*HRA 1998*

'Impact [of HRA 1998] on organisation likely to be considerable. However, not our area of responsibility';

'Not involved to any high degree with the Human Rights Act'.

### 6.2.2 Conclusions

The questionnaire survey provided a useful template, helping clarify issues and frame questions for the case study interviews. Additionally, it gave a useful indication of compliance with the DPA 1998. Almost all respondents to the survey had nominated members of staff with responsibility for data protection. Most had trained their employees in data protection issues, and had audited their holdings of personal information. Knowledge that these measures were in progress enabled further details to be elicited at case study level. Additionally, the reasons for slow development of policy-making in areas such as subject access requests – where only 32 organisations had formal policies regarding employee access to their own personal data – could be explored in further detail. In some respects, however, the questionnaire data belied the difficulties organisations were facing – for example, in the development of formal policies concerning staff use of email and the internet. Although 100 respondents (93.5%) claimed to have policies in this field, the reality at case study interview was different. Only half those interviewed had developed policies. The majority had encountered problems, with many interviewees highlighting frustration over delays in finalising relevant sections of the *Employment Practices Data Protection Code* – intended as the official guidance in this field - and confusion at its interface with the *LBPR* as reasons for lack of policy development. Many practitioners were waiting for strong case law in this field before acting, fearful of being caught in a legal quagmire.

Awareness of the legislation and official guidance was generally high. Most respondents supported the intentions of the DPA 1998 as a positive measure for ensuring compliance and good practice. Nevertheless, comments in answer to question 15 revealed problems existed with the Act itself, which 'does leave so much undefined'. This led to a reliance on strong guidance from the OIC in particular, at least until case law had filled in many of the gaps. Opinion concerning official guidance was mixed. Many practitioners were clearly frustrated – some expressed this dissatisfaction in answer to question 15, others at case study interview. The case studies are analysed in the next Chapter.

## References and Notes

[1] The Article 29 committee are a working party established under Article 29 of Directive 95/46/EC to give advice to the Commission on issues relating to the implementation of the Directive. For EU working papers, refer URL: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm [Accessed 16/01/03].

[2] The two *Codes of Practice* are:

- Great Britain. Office of the Data Protection Commissioner. *CCTV Code of Practice*, 2000;
- Great Britain. Office of the Data Protection Commissioner. *Draft Code of Practice: The use of personal data in employer/employee relationships*, 2000.

[3] Great Britain. Lord Chancellor's Department. *Data Protection Act 1998: post-implementation appraisal. Summary of responses, 2001.* URL: http://www.lcd.gov.uk/ccpd/dparesp.htm [Accessed 16/01/03].

[4] Interview with Hazel Grant, Bird and Bird. London, 02/05/02.

[5] *Ibid.*

[6] European Communities. Commission. DG Internal Market. *Opinion 8/2001 on the processing of personal data in the employment context.* Adopted 13/09/01. (5062/01/EN/Final). WP 48.

[7] Office of the Data Protection Commissioner. *Draft Code of Practice*, ref. 2.

[8] Interview with Data Protection Unit, DG Internal Market, European Commission. Brussels, 19/09/01.

[9] *Ibid.*

[10] European Communities. Commission. *Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.* Official Journal of the European Communities. No. L281/31. (23/11/95). Article 30 (2) states:

- 'If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission immediately.'

[11] Interview with Data Protection Unit, ref. 8.

[12] UNICE. *UNICE position on Commission's first stage consultation on the protection of worker's personal data.* Brussels, 30/10/01.

[13] *Ibid.*, para. 22.

[14] Written answer by UNICE, 06/12/01.

[15] *Ibid.*

[16] European Communities. Commission Press Room. *Data protection at work: Commission proposes new EU framework to European social partners.* Brussels, 31/10/02. (IP/02/1593).

[17] Anna Diamantopoulou, European Commissioner for Employment and Social Affairs, quoted in *ibid.*

[18] Additionally, two other drivers were cited:

(i) *Technological advance.* Examples included: emails; electronic files; the emergence of 'telework', blurring the boundary between private and work life; and cheaper genetic testing technology;

(ii) *Post-11 September insecurity.* This has resulted in some jurisdictions increasing the monitoring of workers or prospective workers as part of broader government efforts to combat the threat of terrorism.

[19] *Data protection at work*, ref. 16.

[20] UNICE. *Commission's second-stage consulation on the protection of workers' personal data. UNICE's reply.* Brussels, 06/01/03.

[21] Interview with strategic policy officer, OIC. Wilmslow, 24/09/01.

[22] *Ibid.*

[23] Interview with Hazel Grant, ref. 4.

[24] *Ibid.*

[25] *Ibid.*

[26] *Ibid.*

[27] *Ibid.*

[28] Interview with CBI. London, 07/11/01.

[29] Interview with MSF. London, 16/10/01.

[30] *Ibid.*

[31] *Ibid.*

[32] Interview with Hannah Reed, Employment Rights Officer, TUC. London, 18/10/01.

[33] The Advisory, Conciliation and Arbitration Service (ACAS) aim to prevent and resolve problems between employers and their workforces.

[34] Interview with Hannah Reed, ref. 32.

[35] *Ibid.*

[36] The UK's largest public sector trade union.

[37] Interview with Hannah Reed, ref. 32.

[38] Reed referred to the *Information and Consultation Directive*, under negotiation at the time of interview (October 2001). The Directive was finally published in the Official Journal of the European Communities on 23 March 2002. When fully enacted, it will extend rights to be informed and consulted in all businesses with 50 or more employees. For text of Directive, refer:

- European Communities. *Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting*

*employees in the European Community.* Official Journal of the European Communities. No. L 80/29. (23.02.2002).

[39] Both are available at URL: http://www.msf-itpa.org.uk/issues.shtml#onlinerights [Accessed 16/01/03].

[40] Interview with MSF, ref. 29.

[41] Interview with CBI, ref. 28.

[42] Interview with Data Protection Unit, ref. 8.

[43] *Ibid.*

[44] European Communities. Commission. *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce.* Brussels, 13/02/02. SEC (2002) 196. URL: http://europa.eu.int/comm/internal_market/en/dataprot/news/index.htm [Accessed 16/01/03].

[45] Interview with CBI, ref. 28.

[46] Written answer by UNICE, ref. 14.

[47] Interview with Hazel Grant, ref. 4.

[48] *Ibid.*

[49] Generally, 'joined-up government' means co-ordinating actions so that different parts of government work in a consistent and coherent way towards the same overall objectives, and in particular making sure that initiatives in one field support rather than undermine those in others.

[50] Office of e-Envoy website, URL: http://www.e-envoy.gov.uk/oee/oee.nsf/sections/index/$file/index.htm [Accessed 16/01/03].

[51] Great Britain. Cabinet Office. Office of the e-Envoy. *Trust charter for electronic service delivery*, 2001.

[52] Interview with Office of the e-Envoy, Cabinet Office. London, 17/10/01.

[53] *Trust charter*, ref. 51, p.6.

[54] Great Britain. Cabinet Office. Performance and Innovation Unit. *Privacy and data-sharing: the way forward for public services*, 2002.

Controversially, the revised 'Charter' allowed for personal data to be processed without the individual's knowledge under a wider variety of broad circumstances, including 'statistical analysis, the protection of the economy, the prevention of crime and disorder, the protection of health or morals, or the prevention of rights and freedoms of others'.

[55] Consumers International. *Privacy@net: an international comparative study of privacy on the internet*, 2001. (URL: http://www.consumersinternational.org/) (Search under 'Publications'). [Accessed 16/01/03].

[56] *Ibid.*, p.42. The five tips given are:

(i) Limit the disclosure of your personal information;
(ii) Set up a separate email account;
(iii) Reject cookies;
(iv) Use tools to protect privacy;
(v) Learn about your legal protections.

[57] *Ibid.*, p.9.

[58] Interview with Consumers International. London, 25/10/01.

[59] Interview with JUSTICE. London, 06/11/01.

[60] Interview with Professor David Feldman, Joint Committee on Human Rights, Houses of Parliament. London, 06/11/02.

[61] Interview with Hazel Grant, ref. 4.

[62] Charity working with disabled people.

[63] Interview with Lord Chancellor's Department. London, 09/10/01.

[64] The example of Canada was given in the interview. In that case, a dispute between the two Commissioners (representing freedom of information and privacy) ended up in the courts.

[65] Refer to discussion in Chapter 5, section 5.4.1.

[66] Interview with CFOI. London, 07/11/01.

[67] *Ibid.*

[68] Interview with the legal advisor to the European Union Committee, House of Lords. London, 08/10/01.

[69] Interview with strategic policy officer, OIC, ref. 21.

[70] Travis, A. Blunkett puts his cards on the table. The Guardian, 04/07/02, p.6.

[71] Interview with strategic policy officer, OIC, ref. 21.

[72] Carter, H. Used in Europe since the last century. *The Guardian*, 04/07/02, p.6.

[73] BBC News Online. Blunkett backs ID card plan. *BBC News Online*, 04/07/02. URL: http://news.bbc.co.uk/1/hi/uk_politics/2084860.stm [Accessed 16/01/03].

[74] Great Britain. Home Office. *Entitlement cards and identity fraud: a consultation paper*. July 2002, p.9. (CM 5557). URL: http://www.homeoffice.gov.uk/cpd/entitlement_cards.pdf [Accessed 16/01/03].

[75] Interview with Professor David Feldman, ref. 60.

[76] *Ibid.*

[77] It remains under discussion. Refer Chapter 5 (section 5.5).

[78] Interview with CBI, ref. 28.

[79] At the time of drafting the Data Protection Bill, the Home Office took the view that the courts 'know what consent means', thus rendering a definition unnecessary. Refer:

- Carey, P. *Data protection in the UK*, 2000, p. 39.

[80] Source: Lord Chancellor's Department. Refer URL: http://www.lcd.gov.uk/ccpd/dpsubleg.htm [Accessed 16/01/03].

[81] UNICE. *UNICE position on Commission's first stage consultation*, ref. 12.

[82] For further details, refer URL: http://www.bsi-global.com/Business+Solutions/Infosec/index.xalter [Accessed 16/01/03].

[83] Office of the Data Protection Commissioner. *Draft Code of Practice*, ref. 2.

[84] Office of the Information Commissioner. *Employment Practices Data Protection Code: Part 3 – Monitoring at Work*, 2002, p. 19.

[85] Refer to debate in Chapter 3: Literature Review, and Chapter 5: Safeguarding data protection: the wider legal context.

# 7. Findings: case studies

This Chapter presents a detailed analysis of findings from the case study interviews. The methodology behind the techniques chosen was discussed in detail in Chapter 2.

## 7.1 Introduction

The case study interviews were devised to assess compliance with the DPA 1998 among public organisations. The intention of the interviews was to test hypothesis 1:

> At an organisational level, the DPA 98 represents a positive measure for ensuring compliance and good practice.

A common approach was taken to all organisations involved. The substantive background to the case studies analysed the nature of the organisations: in particular, their corporate structure and need to process personal data. Additionally, consideration was given to the population each public organisation served. The interviews explored questions raised by those affected by the legislation on a day-to-day basis. The emphasis was placed on detail, with clear examples given of any particular measures enacted to ensure protection of personal data. Attention was given to policy-making within the organisations, in particular how organisational processes were adapted in order to ensure compliance with obligations under the DPA 1998. For ease of reference, the phrase 'Data Protection Officer' ('DPO') is used to refer to the individual in the organisation responsible for data protection, irrespective of their actual job title. Unless otherwise stated, it was the DPOs who were interviewed in the case study organisations.

### 7.1.1 Nature of organisations studied

A total of 18 public organisations participated in the case studies, with one organisation withdrawing shortly before interview. They comprised: 12 local authorities; three universities; one health authority; one police authority; and one 'other' – a central government educational organisation. Prior to interview, all participants – individuals and the organisations they worked for - were promised anonymity. This facilitated some frank discussions not only concerning the workability of the DPA 1998, but also the shortcomings in certain organisations.

The functions and roles of the organisations varied considerably. The greatest number of interviewees came from local authorities. Local government in the UK is structured in two contrasting ways. In Scotland, Wales and parts of England, a single tier 'all purpose' council is responsible for all local authority functions. The 'all purpose' councils comprise unitary authorities[1], metropolitan authorities[2] and London boroughs. The remainder of England has a two-tier system, in which two separate councils divide responsibilities between county and district councils. The 12 local authorities interviewed, included:

- *Eight single-tier councils*: one unitary authority, five metropolitan councils and two London boroughs. They performed a wide range of local government functions including environmental health, housing, leisure, education and social services. The size of the single-tier councils varied widely - from a unitary authority serving a town and its surrounding area, to councils responsible for large cities. Within the eight councils, the number of employees ranged from 3 200 at the lowest end up to 15 000 at the largest Council. The population served in the eight councils varied between 110 000 and 320 000;

- *Four two-tier councils*: two county councils and two district councils. The county councils were responsible for providing services for the whole county, such as education, transport and social services. Both county councils visited employed a large number of staff (24 000 and 30 000) and served a populations of 650 000 and 750 000 respectively. The district councils were

smaller, exercising some autonomy in providing some local services such as housing and environmental health for a specific area within a county. The organisations visited employed 220 and 400 staff, and served populations of 38 000 and 160 000 respectively.

The data protection issues in such diverse organisations, offering a wide range of services, were immense. As one DPO stated:

> "Almost everything one does – in a local authority certainly - has got something to do with people. If you like, the Data Protection Act applies to everything you're doing."

One of the greatest barriers facing the DPOs interviewed was that information tended to be highly departmentalised, with each local authority department having their own subject access procedures, security standards and retention periods for records. Frequently, no comprehensive record existed of personal data held by the organisation. Thus, duplication of personal data was inevitable. This was of concern considering the highly sensitive nature of some of the personal data held by many authorities, especially records relating to social services and education. There was a need for centralised corporate standards. Development of corporate data protection policies and procedures was occurring in the case study organisations, but the rate of progress varied enormously.

Other issues mentioned included: the time and resources involved in training large numbers of staff; sharing personal data with other agencies such as the Inland Revenue and the NHS; and the relationship between data protection and e-Government, with the latter promoting transparency and availability of information.

The three participating universities comprised:

- An established research-orientated university, attracting students from around the world. This institution had 7 500 students – over half from overseas, and employed 2 000 academic and non-academic staff;

- A former college, and a founding member of a large university. This organisation had an intake of 7 000 students and employed 2 500 academic and non-academic staff;
- A former polytechnic, now a vocational university. It attracted 18 500 students and employed 1 500 staff.

A key issue cited by interviewees working in the universities was low level of interest shown in data protection by academics, with many absent from training sessions. The sensitive role of many academics as personal tutors made this an important concern. As in the local authorities, there was a fundamental need to embed data protection awareness into the corporate structure of the university. One DPO described his role as: "Getting everybody to understand: "Think data protection if data on individuals is involved."" Additionally, concerns were expressed about the security of staff information with the publishing of staff email directories on the internet. Resources – an issue with almost all interviewees – appeared to be particularly lacking in the universities, with two of the three organisations interviewed not having a separate budget for data protection.

The health authority interviewed employed 80 staff serving a population of 250 000. Its role was to look after the public health of the community by providing and monitoring services such as general practitioners, ophthalmologists, dentists and pharmacists. In addition, the health authority held the patient information to which the GPs were linked, and was responsible for ensuring that all GPs had Information Management and Technology (IM&T[3]) systems. In this particular health authority, the DPO's main difficulties concerned attitudes of colleagues – especially at board level:

> "Nobody sees [data protection] as a priority. The issue is that I cannot get knowledge improved because nobody sees it as important."

This indifference towards data protection hindered the work of the DPO, and distracted from pressing issues surrounding access to, and release of, sensitive personal data relating to data subjects' health. Although efforts have been made by the DPO to provide staff training, this had not been supported by staff, and

turnout had been poor. In addition, the DPO had received no support in creating policies, staff had abused the computerised patient information system, and no additional finance had been provided for data protection issues. At interview, the DPO was pressing for an internal audit on data protection: "until there's an audit, nobody's going to take us seriously".

The police authority employed 3 500 staff, and was responsible for overseeing policing for a population of a little over one million. The key issues for the DPO concerned fair obtaining of information, ensuring personal data is used solely for its intended purpose, and security of what is often highly sensitive information. Difficulties encountered by the force DPO included the temptation for the police authority keep "forever" any data acquired, for example car registration plates captured by roadside cameras "...because that's intelligence, and that's good intelligence." This was compounded by the motivation of officers wanting to generally "get around" the Act:

> "To me, it's not how you "get around" the Act, it's "how do we deal with the issue in order to comply with it?" That's an entirely different mindset in that context."

Additional difficulties experienced by the DPO included establishing retention periods for personal data that had previously been kept on manual records in order to avoid the provisions of the DPA 1984. Finally, the delays in the establishment of the Criminal Records Bureau had resulted in the police authority struggling with a large number of subject access requests (SARs).

The final case study organisation interviewed differed in that it was global. The organisation employed 7 000 staff in 210 offices across 109 countries. Established by central government, its main purpose was twofold: to promote learning overseas; and to develop relations between overseas countries and the UK. The key issues mentioned by the DPO were data collection notices - informing data subjects of the purpose of data collection - and contracts with external suppliers or even governments:

> "...who themselves wouldn't necessarily recognise data protection and humans rights as the main issues that they want to think about."

This ensured that one of the greatest difficulties faced by this organisation was overcoming overseas resistance as: "they don't see why UK legislation should have anything to do with them." However, because this institution was constituted in the UK, the hierarchy had to ensure the offices abroad were totally compliant with the law. Coupled with this was gaining acknowledgement that data protection was a serious issue – a problem faced by most of the other, exclusively UK, case study organisations. Finally, there were the "ongoing" issues of resources and staffing – again, a typical concern for the case study bodies.

### 7.1.2 Criteria for compliance

The case study interviews were conducted from late February to May 2002. Based on desk research, and findings from the questionnaire survey and expert interviews, criteria for compliance were devised - divided into the following five categories:

(i) *Status of the data protection function* in the organisation: are the DPOs in a position of influence?

The position of the DPO in the organisational hierarchy was mentioned in much of the guidance issued by the OIC relating to data protection[4]. Moreover, the inclusion of this category is justified by recommendation 7 of the Performance and Innovation Unit's *Privacy and data-sharing* report, published in April 2002, halfway though the author's case study interviews:

> 'All public sector organisations should have a named *senior* manager with clear responsibility for the handling of personal information'[5]. [Author's italics].

The word 'senior' reflected the importance central government is now attaching to the issue of data protection. The intention is to discover how far this had filtered down to organisational level. In addition to hierarchy, attention is given to:

- Available training for the postholder;
- Staffing and resources;
- Access to the executive;
- Influence on policy-making.

(ii) *Public awareness*: informing those outside the organisation of their rights under the DPA 1998 at point of collection.

As the authorities interviewed collected personal data directly from their clients and employees, it is important that the data subjects are made aware of their rights at the point of collection. Thus, the need to inform individuals about the way their personal data is handled and their rights under the DPA 1998. Specific criteria include:

- The drafting of a *Fair Processing Code* outlining individual rights and organisational responsibilities;
- Standard statements on forms requesting personal data;
- Training of frontline staff;
- Production of leaflets and posters to inform data subjects.

Finally, the attitude of the interviewees to this task is noted – in particular whether it is perceived as part of their public duty, or as an additional burden.

(iii) *Staff awareness and training.*

This category is clearly significant because without employees handling personal data being trained, organisations are unable to conduct their obligations under the DPA 1998. Criteria include:

- Training methods adopted;
- The extent to which training matched the job descriptions of the employees;
- The establishment of a training culture, sustaining interest in data protection issues throughout the staff member's term of employment.

Finally, some sector-specific difficulties are highlighted.

(iv) *Handling subject access requests (SARs).*

This is the key aspect of the DPA 1998 in allowing individuals to exercise their rights – verifying what is recorded about them and the basis of decisions taken. Specifically, this category sought to answer the question: how do organisations handle requests from both employees *and* clients for personal information? The relationship between employee and client – outlined in Chapter 1 – is particularly important in this context, as both are data subjects for the purposes of the DPA 1998. Moreover, as employees will be handling data belonging to colleagues, it is vital that adequate security arrangements are in place. As security forms part of the organisation's policy-making, it is considered in greater detail in final category for compliance.

In terms of handling of SARs, one key criterion is the existence and content of SAR procedures – in particular the extent to which SARs were documented. A further indicator is the volume of requests received – testing the procedures in place. Finally, consideration is given to whether organisations charged for SARs – employee or client – and the perceived effects of charging data subjects for access to their personal information.

(v) *Data protection policy.*

This category sought to answer the following four questions:

- Do organisations have an overarching policy?
- How effective is it?
- What guidance underpins the policy?

- How is policy evaluated?

Policy is perceived as important for two reasons. Firstly, in stating the organisation's intention to comply with the DPA 1998. Secondly, in order to outline exactly *how* the organisation intends to comply with the Act. Particular attention is given to the security of personal data, with a number of interviewees in the process of integrating data protection into a more wide-ranging information security policy. Finally, this category considered use of employee personal data – particularly that gathered through monitoring of email and internet usage, as practitioners had expressed concerns in that regard during the questionnaire survey. In assessing this category of compliance, emphasis will be placed on the extent data protection had been 'built-in' to other organisational policies – crucial in considering how far organisations were determined to develop a culture of compliance.

The remainder of the Chapter will analyse how close organisations are to meeting the above criteria for compliance. Conclusions will then be drawn about the development of data protection policy in public organisations.

## 7.2 Status of data protection function

This section assesses the key changes to the post of DPO since 1998, the resources and staffing available, any specialist training provided for the DPO, and the location of the post within the organisational hierarchy.

In almost all the case study organisations, the data protection function had been upgraded to some extent. Prior to 1998, data protection was generally a low status clerical post. It was an add-on to a job, usually located in information technology (IT) services, and with little or no budget. Often, the postholder merely processed registrations, "a post-box type situation". A degree of training was generally provided following the enactment of 1984 Act, yet it was allowed to lapse. Since 1998, however, the data protection function has evolved into more of a managerial

post, sometimes with a specific budget. This process was ongoing at the time of interview. To quote a DPO in a large metropolitan council:

> "...it's more structured, more disciplined and more built-in to the way of working. At least it should be when we've finished. Whereas the old Act was tokenism!"

Nevertheless, some DPOs were more pragmatic about their roles. One interviewee, based in a district council, described data protection as "important, but low priority":

> "...we don't want it [the DPA] to be seen as an obstacle that stops us doing the things we're being measured on. We are not being measured on compliance with the DPA. We are being measured on our e-Government agendas."

In this particular organisation, there had been a lack of support from higher up in the organisation. A previous manager had dismissed the DPA 1998 as "legislation which should have been put down at birth", and the interviewee had been working with his current manager for approximately six weeks and data protection had yet to be discussed: "I suspect that speaks volumes really". Another DPO at a metropolitan council had experienced difficulties because she had only been in the post for three weeks and, as the post was graded below managerial, certain managers had not been listening or taking data protection seriously. However, this DPO did benefit from the support of her immediate line manager. Other interviewees had experienced similar difficulties in the immediate time following the enactment of 1998 Act. As status – and knowledge of data protection - had been so low under the 1984 Act, senior mangers would still not turn up for training. However, that attitude was beginning to change, and most DPOs stated that they were listened to by their senior managers. Finally, DPOs found that their role was being boosted by the impending Freedom of Information Act (FOIA) 2000. Indeed, many interviewees perceived FOIA 2000 as the key issue in their role requiring further development. The majority had been given responsibility for ensuring their organisations were compliant with the new legislation, broadening

their task to a records management function – considering all aspects of information handling. To quote an interviewee in a county council:

> "I think there's a need to pull everything together, particularly with the FOIA requirements, so that we have a central policy on retention allowing everybody that needs to, to know a particular type of record."

Within the case study organisations, the role of DPO was generally perceived as middle or senior management, often reporting directly to the Chief Executive or equivalent. Although the posts were not usually full-time data protection, they were permanent and combined with other related duties such as information security and freedom of information. One DPO from a county council saw ongoing training of all employees as more important than whether the post was categorised as 'data protection':

> "My fear with organisations that do have somebody who's labelled 'DPO' is that tends to be a cop-out. What then happens is that the whole organisation says: "Oh well, we don't need to worry about data protection because we've got a DPO", and that can actually be counter-productive."

The important tasks were raising awareness, training staff and establishing contacts throughout the organisation. However, the reverse of this was the experience of another county council that lacked an appointed DPO. That organisation was unusual in that they had an appointed DPO – albeit at a low level – prior to 1998, who had been allocated a small training budget. However, following the DPO's departure in 1997 the post was allowed to lapse, leaving the county council in the position of not having anyone dealing with data protection. At the time of interview, a personnel manager in Corporate Resources was spending less than 10% of his time on the issue. Nevertheless, the case for a new postholder was being discussed, and the interviewees felt it had to be managerial post, answerable to someone of some influence, for example Deputy Chief Executive. A job description and budget made available for new DPO – which had the support of Chief Executive – but it needed to be "brought up priority list". In some respects, this organisation had the advantage of starting with a clean slate.

The training, available staffing and resources, and location of the data protection function could be moulded to suit the particular data protection requirements of that organisation. The remainder of this section considers these three factors are considered in turn.

### 7.2.1 Training

Specialist training was generally provided for the DPOs, frequently resulting in a recognised qualification. Approximately one third of the interviewees had trained, or were in the process of training, for the Information Systems Examination Board (ISEB) certificate in data protection[6]. Part of the British Computer Society, the ISEB provides industry-recognised qualifications in various information systems related disciplines. The training is conducted by accredited training providers such as Masons solicitors. The syllabus comprises 40 hours of course work, including:

- The broad context of the DPA 1998, its origins and reasons for data protection legislation;
- The concepts and elements of the DPA 1998, for example, definitions, the principles, and exemptions;
- Case studies into how the Act works in practice;
- An overview of related legislation.

As an interviewee in a metropolitan council, who was about to study for the qualification, reported:

> "It's becoming a profession now. It's not just a tag onto someone else's job".

In local authorities, the majority of DPOs had been on external training courses, received funding to attend conferences and seminars, and many were members of the professional body, the National Association of Data Protection Officers (NADPO). In smaller organisations, external training was not so extensive, but funds were still available on request. Frequently, the DPOs would supplement

external training with membership of mailing lists such as JISCmail data protection discussion list, and their own reading. Generally, there was a very high level of awareness among DPOs of their training needs, and knowledge of how to pursue them. All had access to legal advice, although it was frequently a case of in-house lawyers approaching the DPOs for advice, rather than vice versa.

Experience in case study organisations other than local authorities, was mixed. In the police authority, external training was available, with the DPO's assistant training for the ISEB certificate. However, the DPO himself had been denied training since 1998. This was in part due to his intention to retire, but mainly a consequence of "the issues and the strategy I've taken as an individual", which involved whistleblowing "within the correct channels...but it doesn't make you at all popular". In the health authority, external training was available, but the expense of some of the courses available sometimes made it difficult for the DPO to justify. In the three universities, external courses were available and funded, although none of the interviewees had studied for qualifications such as the ISEB certificate. Finally, in the central government education organisation there were one-day courses available on data protection and freedom of information. Additionally, the DPO has access to outside law firms such as Bird and Bird and Masons.

### 7.2.2 Staffing and resources

The majority of DPOs had staffing support to some degree. This varied: from the creation of full-time posts of assistant DPOs in two metropolitan councils and the police authority; to temporary staff in other local authorities; to reliance on Data Protection Representatives (or Reps) in the majority of case study organisations. The data protection reps existed in almost all organisations. An add-on to their normal jobs, the Data Protection Reps were responsible for data protection within their particular departments. Their role was usually twofold:

(i) Promote staff awareness of the DPA 1998 in their department;

(ii) Be the first point of contact regarding SARs, responsible for gathering information at ground level.

The role in the SAR process is an important one, and will be discussed later in section 7.5 of this Chapter.

However, data protection reps were not universal, nor were they judged to be completely successful. The Data Protection Rep situation had "lapsed" in the county council without a DPO. In the Police Authority, the DPO had let the reps "die" due to the difficulty in maintaining interest, coupled with the fact that responsibility data protection was being placed on people lower down in the organisation, who had less influence. Finally, one university interviewed did not have a system of reps established.

In terms of resources, six of the 18 organisations allocated a specific budget for data protection, including four local authorities. This fund was used for training, publications and printing. Where the amount was disclosed, it ranged from £10 000 a year to a more paltry £75 a year. However, these figures are misleading as the latter amount related solely to the notification fee. At the time of interview (April 2002), the DPO in the latter organisation had, in the current financial year, "overspent by £10 000, but that's yielded results". Just one university had a budget, of £3 000, to spend on training and printing, although legal advice was funded by the Registrar. The police and health authorities did not have allocated data protection budgets. However, the education body did have a fund to promote data protection. To quote the DPO:

> "It's quite high at the moment, because we're rolling out. But I don't know what it will be next year, and that will have to be negotiated."

In cases where there was not a dedicated data protection budget, further finance was often available if a strong enough case could be demonstrated. Indeed, a DPO in a county council declared himself "quite happy with the resourcing I get", whilst another interviewee based in a London borough stated: "I've never had any difficulty if I can prove that I need some money for my job."

However, other organisations were less happy with their state of funding. An interviewee at another London borough stated that data protection "isn't as well resourced as it ought to be", and a DPO in a small district council complained about the lack of separate provision for data protection:

> "...any training we have comes out of our own Department budget, which I don't think is very fair. But there we are."

Nevertheless, these organisations were in a minority.

### 7.2.3 Location of data protection function

The diverse nature of the DPO role ensured that its placement in the organisational structure was highly problematic, and often the subject of much debate. This was particularly the case in the local authorities conducting wide-ranging functions. Under the DPA 1984, applicable to computerised records, the vast majority of organisations had placed the data protection function under IT. Following the enactment of the DPA 1998, with its implications for all information – manual and computerised – and ensuing concerns regarding the interface with FOIA 2000, many interviewees felt that location in IT was no longer appropriate.

Within the 11 local authorities that had a nominated member of staff with responsibility for data protection, eight placed the DPO function within major policy-making department in the local authority. The name of such a department differed from council to council, variously referred to as 'Corporate Services', 'Chief Executive's Department', 'Central Services' and 'Strategic Services'. Most interviewees believed the data protection function was best suited to this location, as it enabled the postholder to gain the necessary corporate overview required to strive for data protection compliance. Additionally, legal services and central IT services were often located within central corporate department, providing resources for the DPO to draw on. Furthermore, such a centralised location enabled DPOs to be kept "in the loop" regarding projects and systems.

Finally, there was a view that this location helped give the DPO more authority. As a DPO in a unitary authority stated:

> "With DP placed in Corporate Services I don't get ignored like I did when I worked in IT in other authorities. If Corporate Services says it needs to be done it gets done!"

IT and Finance – often the traditional location of DPOs - were perceived by most interviewees to be unsuitable as they were specialist areas. Only three of the 11 councils had the DPO function located within those departments. However, a few DPOs differed in opinion. A practitioner based in a metropolitan council elected - in spite of selling data protection as a corporate responsibility – to be located in ICT Services (part of the Finance Department) for "ease of implementation" as the infrastructure was already in place. The DPO found it easier to get his message across in the form of briefing papers, ICT newsletters and messages of the day, as well as establishing an Intranet website and having immediate technical support. For the interviewee, the Chief Executive's Department would have been "very lonely", whilst access to the Chief Executive was still guaranteed in ICT Services via the Chief Finance Officer.

Data protection in two of the universities interviewed was located in Information or ICT Services. One DPO post was funded by the Registry, thus having links across the entire University network. The DPO postholder in the other university, however, was unhappy with his location in ICT as "data protection is about more than just computerised information". The third university had data protection located in Central Administration – with responsibility shared between the Deputy Registrar and the Records Manager. In the education organisation, data protection was located in Corporate IT.

In the police authority, the location of the data protection post was unsettled. Over a number of years, the function had moved from IT to Quality Services to, at the time of interview, the Professional Standards Unit. The DPO recognised that data protection "doesn't sit comfortably in any role within the organisation because its breadth and all the issues that arise from it". However, he stated there

were conflicts in locating the post in a Unit designed to assure the "professional *integrity* of the organisation – not to assure the professional standards of the organisation" [interviewee's emphasis]. The subtle difference between maintaining standards and merely integrity came "if you find something messy":

> "If you're maintaining merely the professional integrity, some of maintaining that can involve danger."

Whereas, if the police authority was upholding the professional standards of the organisation internally, the implication was that if "something messy" was found, it would be easier to blow the whistle.

Another public authority experiencing difficulties with the location of the data protection function was the health authority. The DPO's official job title at that organisation was *Caldicott* Project Manager[7], with additional responsibility for data protection and BS 7799 – the British Standard for *Information security management*. The post was located in Information, "quite a poor relation" and a subsection of Finance:

> "I answer to a director, but I don't consider that my status is what it should be... I think I've done enough – when I look at other people earning the same as me, and what they turn out... Therefore the influence I have, because of the status I have, is dreadful."

As the interviewee's organisation lacked legal knowledge on data protection, the DPO turned to DPO's in other organisations, particularly the local council, for advice. The essential problem was lack of support from senior management or Directors. Each department in the organisation did have a Data Protection Rep, and a Working Group had been established. However, the people appointed in those positions, in spite of their best efforts, "aren't of status to influence".

## 7.3 Public awareness

Most organisations interviewed were positive about their duty in raising awareness of those data subjects outside the organisation of their rights under the DPA 1998. This issue particularly affected local authorities collecting various personal data concerning council tax forms, applications for bus passes, membership of public libraries, housing tenancy details and so on. At the most basic level, nearly all local authorities included a standard statement on all forms requesting personal data, stating that under the DPA 1998, individuals had rights to access, correction and deletion. A few forms referred to data-sharing that may take place between departments and included contact details of the DPO. Most job application forms stated uses that personal data collected would be put to.

A few organisations went further in raising public awareness. One metropolitan council had drafted a *Fair Processing Code* setting out how the council should obtain information from data subjects. Although use of intranet was popular to raise staff awareness of the DPA 1998, at the time of interview only four of the case study organisations had information concerning the Act on their internet websites. The organisations comprised two metropolitan councils and a university. The information published on the internet included details about subject access rights, contact details for the organisational DPO and a link to the OIC website. The university website additionally included downloads of SAR forms and the university's *Data Protection Handbook*, in addition to a statement concerning sensitive data. However, three further local authorities, at interview, stated their intention to transfer their data protection websites from internal intranets to the internet so most information could be accessed by the public.

More traditional methods of raising public awareness at local authorities included training all front-line staff, and producing leaflets based on the OIC's *Your right to information* to be displayed at all council buildings. Universities incorporated data protection statements on student registration forms and distributed leaflets once a year during registration. One university went a little further, training student union officers in data protection.

However, two public organisations did not perceive their role as raising public awareness. The view of a DPO in one metropolitan council was typical of this minority:

> "It's our job to comply with the DPA, not to make people aware of it – that's the Information Commissioner's responsibility."

A county council went further, justifying their attempts to avoid publicising rights of access stating: "if you try to generate questions, you generate work for yourselves". The county council was a "complex" organisation, and according to the interviewee, the question the council should be asking themselves when it came to publicising data subject rights was: "Is that what we actually want to do?"

Those two organisations were the minority. Most believed that they had a public service duty to raise data protection awareness within the population, although a few stated that the OIC had the greater role in this respect, and that the dry nature of the subject of data protection made the task difficult. As one DPO in another county council confided about his topic:

> "There a lot of very interesting things of course but they're interesting to the likes of you and me. They're not terribly interesting to everyone else..."

## 7.4 Staff awareness and training

Training and the consequent raised levels of awareness among staff are vital if public service organisations are going to be able to demonstrate compliance with the DPA 1998. Indications from case study organisations suggest that staff training was taken very seriously. Development of such training, however, was at various stages. At one end organisations were employing external consultants to research the data protection training requirements, whilst a few organisations had in place a highly organised Corporate training structure: centrally planned, tailored to the needs of employees at various levels in the organisation, and comprehensive

enough to demonstrate considerable efforts had been made in attempting compliance with the DPA 1998.

### 7.4.1 Methods

As discovered in the questionnaire survey analysed in Chapter 6, most training in the case study organisations was conducted in-house, on the initiative of the DPO[8]. The most popular format for introducing staff to the DPA 1998 was presentations by the DPO, enhanced by publication of more detailed information on the corporate intranet. Data protection training was gradually being built into the general induction process for new employees. A few organisations were considering software packages to enhance established training methods. Finally, the nature of training was evolving: from a diverse, department-driven approach, to a more centralised corporate approach - although the often convoluted processes of policy approval hindered progress in this respect.

#### *Staff presentations*

Almost all DPOs had given presentations to the staff concerning the 1998 Act. This in-house training was viewed as the most effective means of reaching a large number of staff quickly and cheaply. The methods varied. In one metropolitan council, the individual departments identified their particular training needs, then reported back to the DPO. The DPO then conducted formal training sessions, which ranged from one hour's awareness to full-day's workshops. The workshops were aimed at departments such as Social Services and Education where there were sensitive data protection issues that required a specific type of awareness. In this authority, the minimum requirement was issuing leaflets for all staff outlining their responsibilities under the DPA 1998 and mounting posters on the council buildings. The DPO measured awareness through the number of hits on the data protection intranet website, "about fifty a week" and any queries received:

> "I'm getting about 30 emails a day. That includes JISCmail – but also quite a few data protection queries, advice and guidance there, plus all the telephone

> calls. So awareness ... has proved to be highly escalated as the training initiatives are getting out."

In another metropolitan council, the DPO had trained 2 500 out of 14 500 staff, with some departments conducting their own training. The DPO's own training involved a two-hour presentation with slide shows and various "tall stories" designed to alleviate the dry subject matter. Additionally, newsletters were published to keep staff informed with latest developments as well as look in detail at one or two key data protection issues. The DPO in the health authority had enjoyed less success. Over a two-year period, the interviewee had conducted two sets of one-hour sessions, and expressed disillusionment that "hardly anybody turned up". The essential difficulty was lack of support from directors and senior management. However, the DPO felt that her brief had been fulfilled:

> "I've got enough evidence now to say: "These were provided, you failed to ensure that staff attended.""

This was an exception. Generally, DPOs in the case study organisations had the full support of those at executive level.

Essentially, the trend was for short one or two hour presentations supplemented with more specialist training on demand. In local authorities, more specific service training was provided for departments such as Housing, Education and Social Services as they dealt with intimate details of people's lives and held the most personal data. A DPO in a unitary authority explained how data protection issues were handled in such circumstances. Joint training with staff from the affected departments addressed issues of confidentiality and pertinent policies. In Social Services departments, access to information can go back 40 years, with people often wishing to know their family background when they were fostered or adopted in order to find their biological parents. Such issues needed to be handled with extreme care. Often, a social worker was on hand to explain and sometimes counselling needed to be offered to the data subject. In such circumstances, a DPO could not just release the personal data to them as it could, in certain

scenarios, cause untold damage. In relevant departments, presentations by a social worker often formed part of the staff training.

*Intranet and video*

The use of the intranet was pervasive, supporting training in almost all organisations interviewed. Typically, a data protection intranet site would include contact details of the DPO, the main provisions of the Act, copies of any policies or guidance drafted by the DPO, a question and answer session for staff to test their data protection knowledge, and contact details for the OIC.

Other methods of raising awareness included use of educational videos. This was less widespread, although three local authorities of varying sizes employed the OIC's public service video, *Barry's Bad Data Day*[9], as a training tool. One metropolitan council posted a streamed version onto its intranet. A London Borough believed the video provided "a bit of levity", working well as staff could relate the office situation outlined to their own workplaces. However, one district council disagreed, believing that if staff did not know anything about the DPA 1998 prior to viewing the video, it would "just pass them by".

*Induction*

At interview, case study organisations were beginning to include data protection training as part of the induction for new starters. Approximately two thirds of institutions interviewed either included data protection as part of the induction process, or were planning to do so in the near future. Typically, at induction, fresh employees would view a short presentation concerning the basic principles of data protection, receive leaflets and various guidance on how to avoid breaching the DPA 1998, and a few would view *Barry's Bad Data Day*. Generally, training at induction was perceived to be the ideal introduction to data protection. However, one DPO in a district council expressed concern about the timing of the induction training:

> "I'm inclined to think that it's maybe too soon for them to absorb everything – data protection along with health and safety and everything else. We need to consider some refreshers because it seems to be something that soon becomes a dim and distant memory...It's an almighty job trying to keep people interested."

*Training packages*

In addition to providing data protection training on corporate intranet, some organisations were researching computerised training packages. The DPO at the police authority had previously considered a software package prior to 1998, but "wasn't impressed". However, he acknowledged the package had been improved since, and suspected "the force will buy one before too long". The DPO in a London Borough was considering computerised training "because I can't get in front of 8 500 people". Additionally data protection was built-in to computer training course modules at the police authority and certain local authorities. For example, a few organisations were incorporating training in software packages such as Microsoft Word and Excel with data protection training, in order to maintain levels of awareness and reinforce the "relevance of data protection to all aspects of information handling". This "integration" could be viewed as part of an overarching policy to filter data protection into organisations' standard corporate procedures. This is discussed further in section 7.6.3 of this Chapter.

### 7.4.2 Targeted training

Maintaining interest was a difficulty cited by many interviewees. Some organisations tried to sustain employee awareness by having more targeted data protection training. One of the best organised is this respect was a metropolitan authority, where training needs were divided into three groups:

(i) *Lower risk*:

This applied to employees not generally in contact with personal data (for example, parks and ground staff). They received a leaflet about the DPA

1998 once a year, and were visited by managers to ensure they were "reasonably confident" about data protection;

(ii) *Average risk*:

This applied to general office staff, who came in routine contact with personal data. They received the guidance above plus intranet training. The intranet training involved an assessment resulting in a score out of one hundred. The test was repeated on an annual basis, thus continually enforcing the training;

(iii) *Management training*:

This was the most targeted training, aimed at managers and those working in fields involving processing of particularly sensitive data (for example, Social Services, Education, Housing, CCTV). This group receive all the instruction outlined above, plus training by an external firm of solicitors.

Another metropolitan authority was considering a similar technique, researching computerised training packages also graded at three levels: executive; middle management; and front-line staff. However, a further metropolitan authority was looking at its training needs according to staff function. In this organisation, the DPO had conducted detailed briefings with the Data Protection Representatives on their role, identifying the key groups that needed training. Customised training was then produced that was "relevant to each group". At the same time, certain sections in the organisation could approach the DPO when they thought there was a significant data protection issue (for example processing CCTV footage).

Some organisations, in particular those in the early stages of data protection compliance, used external consultants. One county council was devising a training plan as part of a consultancy making Best Value recommendations[10] for the organisation. A district council used external consultants for two days' introductory training into data protection, and on the relationship between the DPA 1998, and HRA 1998 and FOIA 2000. Another district council employed the same consultants four times to take "morning and afternoon sessions with 40 to 50 people at one time", and covering most staff.

Regarding the HRA 1998, practitioners appreciated the significance of the Act and most organisations had provided staff briefings. The views of one DPO, based in a metropolitan council, summed up the position of most interviewees:

> "We are aware that the HRA is there, and that it needs promoting. But it is not specific to my job. Data protection and freedom of information are more of a priority."

The key exception to this approach came from the police authority, who, due to the nature of their work, have prepared vigorously for the Act. Nationally, the police had audited existing practices, policies and procedures to identify breaches and potential breaches of Convention rights:

> "There's a great deal on nervousness in the police service on human rights because the HRA is now inclusive, rather than exclusive as in 'if it's not covered by the law, then you are free to please yourself'. It's a significant change for the police service – very significant."

The HRA 1998 was being implemented across the police authority, with a considerable amount of training underway. The interviewee thus found the HRA 1998 "very useful" in bolstering his own work.

### 7.4.3 Difficulties facing local authorities

With their wide-ranging functions, local authorities in particular faced some difficult challenges when training in data protection. Social Services were mentioned in the previous section. Schools and councillors also posed difficulties, due to their legally ambiguous relationships with local authorities. Under the DPA 1998, schools are separate data controllers, responsible for their own notification procedures and legally liable for the data they process. However, many schools were not well versed in data protection issues, with DPOs observing that certain headmasters believed they had complete ownership of information held on record. Notwithstanding this, most local authority DPOs perceived it as

their duty – as the institution responsible for education provision - to provide basic training. One metropolitan authority found that writing to schools about the hazards of non-compliance most effective:

> "I wrote to them last February [2001] – the letter arrived on a Friday morning, and I had 80 phone calls by the Monday night. The phrase 'the headteacher's liable for a £5 000 fine' might have had something to do with it!"

Most DPOs judged their role in relation to schools as one of advising and helping with their notifications and subject access requests. As there was sometimes a need for Social Services to liaise with schools, training on basic records management and access rights acquired huge importance.

The legal position regarding the role of councillors is complex. Councillors can play three roles:

- A member of the council, for instance as a member of a committee. In this case, the councillor is not required to have his or her own data protection notification and is effectively in the same position as an employee;
- A representative of the residents of his or her ward, for instance, in pursuing complaints. In this case, they need to notify in their own right. Most local authorities, whilst accepting this, also accept the only reason they may be involved is because of their Council duties and therefore pay the annual fee and provide help and assistance in becoming notified;
- A representative a political party, particularly at election time. In this role, notification should be the party they represent.

In spite of the legal complexity of data protection in this context, and of most councils' willingness to help, many councillors did not attend training courses. Particularly problematic were issues involving a conflict of interest, especially any use of personal data – for example, relating to individuals eligible for bus passes - for political purposes, as two DPOs in metropolitan councils have experienced:

"Basically having to tell elected members that they shouldn't be doing certain things, one has to treat it very diplomatically!"

"It's been very difficult in the past to get elected members to take any notice. Under the new Act, it's much stronger. We're taking advantage now the elections are here, and the Members are going to have to have training. I've already written the guidelines. I didn't want them to have a huge raft of stuff – just the minimum they needed to know, and then where to come if they've got a problem."

One metropolitan authority at interview was taking legal advice concerning a councillor who asked in writing for personal data from a council survey, which he proposed to use for purposes other than those originally intended. When the interviewee refused, the councillor threatened court action. At the time of interview, the DPO had referred the case to the council's barristers.

### 7.4.4 Towards compliance?

Overall, most case study organisations interviewed were well-advanced with staff training. There were variations between the types of authorities, with local authorities and the police authority tending to be better resourced than universities or the health authority. However, a lot of progress regarding training depended on the status and personality of the DPOs. Most local authorities were well organised, although one county council was at the stage of awaiting recommendations from its consultants. The police authority was in full progress with induction training. Furthermore, data protection manuals had been published for all computer courses, and the DPO had promoted his role by issuing policies and encouraging staff feedback. However, training was not regularly reviewed and data protection considerations were not generally built-in to the IT procurement process - a situation noted by Grant when commenting on public authorities in general in Chapter 6. As the police authority DPO stated, legislative requirements: "need to be addressed from the beginning, not when the risk comes home to roost."

At the health authority, the nature of the problems was similar, but the level was more severe. The DPO's attempt to generate staff interest through presentations had suffered due to poor turnout. However, a CD had been developed to guide staff through the requirements of *Caldicott* and data protection, and help the DPO cope with lack of time and resources. This initiative had largely been successful. In total, 2 000 CDs had been developed, and: "most have gone out. The issue now is – are people using them?"

Training in universities was on the initiative of the DPOs, who appeared more hampered by lack of resources than DPOs in local authorities. Those interviewed had trained the clerical staff through a combination of presentations and provision of handbooks. However, the lack of interest was shown among academics was a concern for DPOs at the three universities interviewed. Finally, training in the education organisation was at a similar stage of development to most of the local authorities. In their UK offices employing 1 200, all but 90 employees have been instructed in data protection. The training has been conducted in-house by the DPO, an induction pack was "being worked on" and contact details for the DPO had been put on the intranet. In many ways this organisation is typical of development in most case study organisations. Basic training has been conducted, and a more structured approach was under development in order to achieve full compliance.

## 7.5 Handling subject access requests (SARs)

Section 7 of the DPA 1998 provides that a data subject is entitled, upon written request, to be informed whether the data controller (the organisation) is processing personal data to which the individual is the data subject. A fee – in most cases subject to the statutory maximum of £10[11] – can be charged by the data controller for this service, and the data controller has 40 days from receipt of the request to comply with it. The 40-day time limit does not start until the data controller has received the fee and/or has been supplied with sufficient information to enable compliance with the request. The right of access is the key right in the data

protection legislation, enabling individuals to request, and verify, information held by organisations concerning them.

### 7.5.1 Procedures

As this was such an important aspect of the DPA 1998, it was not surprising to discover that all but three case study organisations had developed well-defined procedures. Essentially, the process was:

1. Individual would submit the subject access request (SAR) together with proof of identity and a fee if appropriate;
2. This would be checked by the DPO. If the SAR contained sufficient information, the DPO write back to the individual informing them of the 40 day time limit;
3. DPO would send out standard letter to relevant departments asking for personal data. A deadline would be set;
4. Data Protection Reps would gather the personal data, and report back to the DPO;
5. DPO would perform the final checks: to verify, for example, that there was not any data relating to other people without their permission;
6. Despatch personal data to data subject.

The three organisations without working SAR procedures were a county council, a London borough and the health authority. In the two local authorities, procedures were "under development" and expected to be in use within six to 12 months. In the health authority, the DPO admitted the procedures were "something I've got to start working on." At the time of interview (April 2002), no action had been taken – due to lack of time and support. This was mitigated slightly by the fact that health authority did not generally receive SARs from the public. However, the DPO doubted that most staff in the organisation knew they could view their records:

> "It's like data protection is not about them, it's about Joe Public, and when they're at the health authority, they're not Joe Public, so therefore data protection does not apply to them. But it does."

The lack of procedures enabling staff access to their personal data concerned the interviewee, especially in view of certain abuses of personal information that had occurred in the authority. The most serious breaches involved misuse of the computerised Patient Management System, with individuals looking up of details colleagues in hospital and, in one case, discovering that a colleague was pregnant. Such conduct left the DPO "waiting for the day that someone takes out a case – a member of staff against a member of staff".

A complication regarding SARs was establishing procedures for requests for CCTV images. With increased usage of such technology in town and city centres, this was of particular concern for local authorities. It was being addressed, but as a DPO in a metropolitan council stated, progress was slow:

> "It's been dealt with through the whole lengthy process of Committees, and agreements, and ratifying and rubber-stamping."

At the time of interview, requests for CCTV images had not been completely built into most authorities' standard SAR procedures. However, there were exceptions. For example, a small district council had drafted a specific form regarding CCTV requests, had liaised with the Crime Prevention Officer, and established a simple procedure whereby:

1. Initial requests sent to the DPO, who logs them;
2. The SARs then go to the police, who administer entire process;
3. Police inform the DPO once the process was complete.

At the time of interview, the council had not received a SAR relating to CCTV, but the DPO had ensured "all the documentation [was] in place."

### 7.5.2 Volume of SARs

The volume of SARs received was difficult to ascertain as the process was not always documented. At the time of interview, only a few case study organisations had introduced centralised documenting procedures. Most metropolitan councils centrally logged all SARs received on a database. This was partly to keep on top of procedures to ensure deadlines were not missed, in addition to demonstrating compliance with internal performance indicators. Moreover, it ensured that the organisation had evidence of action in case any SARs resulted in litigation.

However, in other organisations the procedures were less rigorously monitored. One metropolitan council chose not to document SARs centrally. The DPO stated:

> "They are actually mostly received at Departmental level, and I haven't actually got figures for that. It works quite well, so I've not tried to change it."

Processing the majority of SARs at departmental level ensured flexibility and speed in dealing with requests in targeted areas such as Social Services and Housing. A DPO at a London borough council took a less official approach to processing complex SARs centrally. Although formal and legally compliant procedures were posted on the corporate intranet, when receiving SARs the DPO preferred to have an "informal chat" with the data subject than follow through the official process with the accompanying red tape:

> "It's better than ending up being cut to pieces by sorting out the bits of paperwork. It's worked effectively for me like that, and I don't want to get forced down the route of a formal process."

All the interviewee required was for the departments to inform his office when they had formal applications. This combination of "informal chat" and formal legal guidelines to refer to if necessary appeared to work very well, although its success was largely to due to the experience and personality of the DPO. The

total number of formal, centrally administered SARs – four received in the previous five months - was small enough for the DPO not to be overwhelmed with "informal chats" to the data subjects.

Indeed, the number of formal SARs processed, where figures were available, was generally very few. In local authorities as a whole, the volume of SARs ranged from six since the DPA 1998 was implemented in March 2000[12] to another organisation receiving 18 in the previous calendar year[13]. The universities received fewer formal requests, with one institution having processed just the one formal SAR since the DPA 1998 came into being. Another university had received three SARs in the same time period – all staff grievances. In the final institution the DPO "heard a year ago we'd have 10 since 1984". Although uncertain whether or not that figure was accurate, it demonstrated that the volume of SARs had been very few indeed, even in institutions employing a large number of staff and serving a sizeable population.

The education organisation had received 10 SARs in 2001. Those requests, like the universities, comprised "grievances, disciplinary issues" and a few who have requested information from the corporate database "out of curiosity". In the health authority, the number of SARs received was unknown, but was "likely to be very small". Indeed, the only organisation to receive a large number of SARs was the police authority. The overwhelming majority received by the police were for convictions history, which in 2001 totalled 2122. They were processed by the authority's Criminal Records Office, Subject Access Bureau. At the time of interview (April 2002), this task was due to be taken over by the Criminal Records Bureau (CRB), the establishment of which had been somewhat delayed[14]. Once the CRB was fully active, the police authority's DPO will only be processing internal SARs from within the police authority's catchment area. However:

> "...the internal [SARs] are growing. I dealt with three or four yesterday, so we're probably now getting to the stage of receiving maybe 10 a week."

The internal requests can relate to sensitive criminal cases occurring within the police authority catchment area or to staff requesting information relating to police

exams after feeling they "were being unfairly passed over". Such internal SARs are processed by the DPO.

### 7.5.3 Charging for subject access

Interviewees were divided on charging for subject access. 12 of the 18 public organisations interviewed did charge for SARs to some extent. Five chose not to, and one organisation – a county council – was "undecided". Those that did charge mainly believed it would be a useful deterrent against frivolous and/or malicious requests. As a DPO in a metropolitan council stated:

> "I use it very much as adding to a negotiating position: "If there is a specific piece of information you want, you can have it free of charge. Or, if you want the whole lot, we can do it for £10.""

Others charged for administrative reasons. Another interviewee, based in a metropolitan council, stated that the £10 charge was used as a "reference point", to avoid entering into debate with data subjects about when the 40-day period began:

> "It's not the money we're interested in, it's getting the procedures right – the point in time when we received it."

Only one case study organisation, a university, stated that charging was used to "cover costs". Frequently, the local authorities that did charge made exceptions, for example, for Social Services records, due to their sensitive nature. Housing records were sometimes exempted from any fee because the data subjects were generally in dispute with the council and, to quote a DPO in a metropolitan council: "charging those on low incomes could be seen as putting a barrier in their way".

The five organisations that chose not to charge at all made their decision as charging would be:

- Against the public service ethos of their organisation;
- Poor public relations;
- An administrative burden. One DPO in a small district council stated: "it'll cost us more to invoice, or whatever, to collect that £10…it's pointless."

Regarding staff access to records, the approach of case study organisations was generally twofold. If an employee requested access to their personnel file, this would be granted free of charge. If employees request more detailed information – such as access to all emails making reference to them – which would involve more time and effort on the part of the organisation, then a formal SAR would have to be submitted, following the same procedures as all other data subjects. Most DPOs were keen to avoid the latter situation. To quote interviewee from a large metropolitan council:

> "We take the view that when [employees] get to the stage of submitting the SAR, it tends to suggest that something's failed somewhere… If our procedures are right, then it should never happen."

Where staff had submitted formal SARs, it was because they were in dispute with their employer, often concerning disciplinary matters or being overlooked for promotion. Such disputes were, in the words of a university DPO:

> "…ongoing issues where they thought by doing the SAR they would gain more information for their cause, if you like."

Staff SAR procedures did differ in the police authority. If a member of staff did not want to explain why they were submitting a request, they submitted a form and paid the police authority's standard £10 fee. If they did not want to pay the fee, the individual would submit a report to the Force requesting the material and explaining the reasons for the request.

The handling of SARs was taken seriously by the DPOs. The majority of case study organisations had written procedures in action, and those that did not were aware of their obligations to data subjects in this respect. Organisations'

willingness to follow their own SAR procedures varied, with some DPOs going by the letter of the law, whilst other practitioners were willing to be more flexible – ringing data subjects up at home in their own time to establish "what they really wanted". Both approaches had merit, and appeared to be successful. Most organisations charged for SARs, although many organisations made exemptions in sensitive cases, or with requests affecting people in lower income brackets.

Whether charging acted as a deterrent to subject access is difficult to state, and was not part of the remit of the interviews. However, the low number of SARs received was surprising, with most case study organisations averaging one formal SAR a month. This did not include SARs dealt with internally by departments such as Social Services and Housing. The exception to this was the police authority, averaging almost 10 'internal' SARs a month. These comprised requests made by employees of the organisation regarding material the organisation processed about them. Out of the criteria measured so far in this Chapter, handling of SARs is perhaps where organisations demonstrated greatest compliance with the DPA 1998. The next section analyses how the criteria measured to date form part a coherent data protection policy for the organisation.

## 7.6 Data Protection Policy

Dictionary definitions refer to policy as the decisions that an organisation makes on the actions it should take. A written policy should describe the basic plan to achieve an agreed course of action. In the case study organisations, policy-making on data protection was frequently represented by two types of document:

- A short clear general statement of the organisation's intention to comply with the DPA 1998;
- Detailed procedures outlining how the organisation would achieve data protection compliance, in fields as diverse as housing policy and email monitoring. Often outlined with targets, and sometimes differing versions aimed at various levels of staff in the organisation.

Some organisations concentrated on the procedures, and did not have the statement of intention. A few were still at the drafting stage, and did not have any concrete data protection policies. Nevertheless, many had both the statement of intention and the detailed procedures. The former was generally a tool to demonstrate compliance, being aimed at the wider audience, including the public and OIC. The detailed procedures frequently took the form of a corporate manual, devised for internal use. This section investigates the influences behind - and then the contents of - data protection policy and procedures. It concludes with an assessment of the extent to which data protection has been built into the general policy-making processes of public organisations, and how the case study organisations evaluate the success of their policies in achieving compliance with the DPA 1998.

### 7.6.1 Influences

In the process of policy development, interviewees took advice from the OIC and their peers, with a considerable degree of cooperation occurring between organisations. In addition, professional bodies in IT, business and law were all consulted. This subsection reviews the key influences cited by interviewees when devising policy.

Many organisations referred to the data protection supervisory authority, the OIC, for initial advice. Although little was provided in terms of model policies, many DPOs found the OIC's written guidance helpful. However, in the words of a DPO working in a large metropolitan council, some practitioners felt the OIC's policy advice tended "to be a bit over-detailed and over-prescriptive at times." In an echo of concerns voiced by the CBI in Chapter 6, the draft *Employment Practices Data Protection Code* was highlighted as potentially "causing serious problems for employers".

The main complaints from DPOs across all sectors interviewed were that the draft *Code* was "daunting", "over-complex" and "a personnel issue". Indeed, many practitioners had delegated interpretation of the *Code* to their personnel offices,

affording the document barely a "cursory glance". Additionally, there was a feeling that draft *Code* was something of a legal minefield, clashing on the issue of monitoring with RIPA 2000 and its *Lawful Business Practice Regulations*. The parts of the *Code* that had been finalised at the time of interview were generally perceived to be "better, but still far too long". Generally, practitioners were underwhelmed. In the view of the DPO in the education organisation:

> "At the moment, sometimes it's not terribly helpful, sometimes it's not terribly clear, and sometimes you think: "Well, we are already doing that anyway.""

A minority of organisations were more positive. A DPO working in county council found the draft *Code* to be "excellent":

> "I actually use it as though it was not a draft, and I've based guidance on it because I think it's reasonable, it's sensible and it strikes a nice middle of the road balance."

Another DPO in a metropolitan council concurred and was in the process of "championing" the document – building it into his organisation's data protection code of practice and into general human resource strategies. Although a minority of DPOs used it as a foundation for policy-making, most did not - being deterred by its length, wide scope and complexity. In many cases, it appeared to be unread, certainly by those working in data protection. This defeated the OIC's stated objective in drafting the *Code* "as a reference document". In this respect, the OIC had trouble in determining its audience.

Nevertheless, other OIC publications were praised. One of the most frequently mentioned by DPOs was the OIC's *Legal Guidance*[15]. Intended by the supervisory authority as a reference document for data controllers and advisors, the *Guidance* provided a broad guide to the DPA 1998 as a whole. It outlined the OIC's view as to how many of the provisions in the Act should be interpreted, and included definitions of terms such as 'personal data', 'processing' and 'data controller'. One DPO, working in a metropolitan council, referred to the

*Guidance* as his "bible" - using it as a basis to answer any queries. That way, if the wrong advice happened to be given:

> "...you've made your best efforts and you've used the most official guidance you can – you can claim extremely mitigating circumstances!"

In the main, the OIC was consulted more to answer specific questions, rather than to assist in devising policy documents. Moreover, the OIC faced the practical difficulties encountered by a publicly funded watchdog, being expected to police a complex piece of legislation on limited resources. Particularly problematic was the exodus of highly trained but poorly paid staff at all levels to financially more rewarding posts in other sectors. During the author's visit to the OIC office in Wilmslow, the interviewee stated that it was not uncommon for skilled Compliance Officers to more than double their existing wage by taking up positions in industry[16]. Whilst it is unlikely that OIC salaries will ever compete with the private sector, it was surprising to find many experienced data protection professionals in Wilmslow earning sometimes significantly less than their counterparts in local government[17].

When actually drafting documentation, the vast majority of interviewees liaised with their peers. In this respect, a few interviewees believed the OIC could make a contribution – acting, in the words of a metropolitan authority DPO, as a "facilitator" between public organisations from different sectors. The sharing of knowledge was particularly strong among DPOs in local authorities, most of whom were members of the National Association of Data Protection Officers (NADPO), a non-profit organisation aimed at promoting the role of public sector DPOs. NADPO is structured into a number of regional groups. During interviews, the West Midlands[18] and London groups appeared particularly active. In the West Midlands, five metropolitan councils created and adopted a joint *Data Protection Code of Practice*[19], discussed in section 7.6.2 below. Two of the case study organisations interviewed were part of the West Midlands group, and interviewees outside of the region had approached the group members for advice. The London group – which included one interviewee as a member - had consulted with Masons' solicitors with a view to providing an online 'information law

service'. This service would be subscription-based and, according to a London borough DPO, provide information concerning "policies, protocols, standards, layouts, documents", plus general computer-based training.

Some of the interviewees from an IT background were members of the Society of Information Technology Management (SOCITM). A professional association for ICT managers working in and for the public sector, SOCITM had a membership that included 90% of all UK local authorities[20]. SOCITM formed a data protection group to provide a forum for members with an interest in the implications of data protection legislation on ICT, with the aim of producing guidance for all members. Three of the DPOs interviewed were members of SOCITM.

Finally, some local authority DPOs drew on the Improvement and Development Agency (IDeA) for policy advice. Established by local government to 'deliver practical solutions to improve local government performance', IDeA enables councils and their employees to create, pool and exchange learning resources on various topics including data protection and freedom of information. Additionally, the Agency's website has downloads of various draft guides and forms, for example, concerning the implications of the DPA 1998 for councillors[21].

In the further and higher education sector, the Joint Information Systems Committee (JISC) is a major forum for exchanging ideas. JISC's role is promote application and use of information systems and information technology in further education and higher education across the UK. Two of the three university DPOs interviewed had referred to *JISC Data Protection Code of Practice*, which JISC had produced with Hull University[22]. JISC hosts the JISCmail data protection discussion list, enabling practitioners and researchers in the field to share information. As a DPO in a university remarked:

> "I certainly view [JISCmail] as the next level down from the OIC, because you can go there and a lot of people have had the same problems and you can see what they did."

In the police authority, the DPO used the Association of Chief Police Officers (ACPO), the professional body for the UK's most senior police officers[23]. ACPO had also produced a draft code of practice on data protection, referred to the OIC for consultation in November 2001[24].

Additionally, interviewees drew on organisations removed from the sectors they were employed in for data protection advice. The British Standard Institute (BSI) was mentioned by the majority of DPOs. In conjunction with experts and the OIC, the BSI has produced the *Guides to the Data Protection Act 1998 (PD0012)*[25], to which a number of case study organisations had subscribed. The *Guides* advise organisations on how to ensure compliance with the DPA 1998 when managing their information processing operations. The first *Guide* concerned the practical implementation of the DPA 1998[26], and others have covered specific fields such as subject access, email policies and manual data. To date (January 2003), nine *Guides* have been produced, with a tenth *Data Protection and Information Security*[27] due later in 2003. Five of DPOs interviewed made reference to the generic *Guide* on practical implementation of the Act, when devising policy. In the words of a DPO in a small district council:

> "I thought it was good actually. It helped to get me going, to be honest, to develop the policy."

In addition to the BSI, case study organisations referred to the National Computing Centre (NCC)[28], an independent membership and research organisation aiming to promote more effective use of information technology. Membership included both public and private sectors. One large metropolitan authority based their data protection policy on the NCC's recommended guidelines[29]. Another reference source was the *Encyclopedia of Data Protection*[30] – a loose-leaf publication bringing together relevant legislation, decisions and codes of practice. The *Encyclopedia* is updated twice a year to keep subscribers informed of latest developments. The DPO based in the police force found it particularly authoritative. Finally, many organisations had consulted law firms for

policy advice, as well as training. The most frequently mentioned were Masons[31] and Bird and Bird[32].

### 7.6.2 Policy development

This subsection analyses policy development in the case study organisations. For ease of reference, each 'type' of authority is considered in turn: local authorities; universities; the health authority; the police authority; and the education body.

#### *Local authorities*

All but two local authorities interviewed had defined policies and procedures in place. The majority of the councils had short policies of one or two sides of A4, supported by detailed guidelines. A metropolitan council had a general statement of intention as an overview. The interviewee stated its aim as simply:

> "safeguarding personal data. We are custodians of personal data. That is the angle we are coming from. We're expected to treat it in an appropriate manner."

This was supplemented – as in another case study organisation – by the West Midlands group's *Data Protection Code of Practice* as a framework. This 160 page document concerned shared best practice between the five large West Midlands councils, and stated its purpose as helping 'the Council'[33] comply with the Data Protection Act 1998.'[34] A collection of 'guidelines and procedures for employees of the Council', it guides employees through the terminology of the Act, the eight data protection principles and their relationship to data handling procedures in the Council and exemptions. Particularly useful for employees is section 9: 'other relevant legislation and links'. This section details issues surrounding the internet, direct marketing, HRA 1998, RIPA 2000 and e-government. This was particularly relevant in ensuring privacy was respected when employee email and internet usage was being monitored. Section 10 – 'commonly asked questions' - is also extremely useful for the novice, and is

probably the first section many employees would refer to. Finally, detailed procedures are outlined in the appendices. The appendices include procedures on:

- Contracts with data processors;
- SARs;
- Information from third parties;
- SARs via third parties;
- Requests to stop processing information;
- Requests to stop automated decision making.

Additionally, the appendices outline specific Council contracts and a number of case studies taken directly from the OIC's website. All in all, this was the most impressive and up to date policy document that had been drafted by the case study organisations. Indeed, the West Midlands group's *Data Protection Code of Practice* included something for all local authorities.

Other councils had variations on this approach. Another metropolitan authority had developed a handbook *Data Protection: guidelines and procedures*, which had been used as evidence to the OIC following a complaint against the Council by a data subject. The document's purpose was to provide 'guidelines to assist in the implementation of [the Council's] data protection policy'. The guidelines were not exhaustive, but provided a framework under which the Council would conduct its normal activities, so that the DPA 1998 was complied with fully. The policy was returned by OIC with only a few minor corrections, leading the DPO to conclude: "if you like, it has got the approval of Commission."

A county council chose a different approach, developing a well-structured, four-tiered policy that integrated data protection into a policy concerning 'information security':

1. *Information Security Policy*
    - This involved short guidance aimed at top level – mainly directors and senior management. It set out the minimum acceptable level of

information security management and the primary responsibilities for information security in the Council.

2. *Information Security Manual*
   - Based on the standard BS 7799, the *Manual* provided a guide for IT practitioners, and could be used as a basis for internal policy or guidance;
   - A substantial document, the *Manual* was constantly revised and updated to reflect changing technology, legislation and official guidance.

3(a) *Supplementary Guidance*
   - Specialist papers, for example on *Internet use monitoring* and *Private email*, published where specific issues required additional guidance. This also included guidance to personnel for handling employee personal data, and ensuring access to such information was strictly limited;
   - Mainly aimed at IT practitioners and managers, but could be of use to other employees seeking information on specific issues concerning information security.

3(b) *Departmental Information Security Guidelines*
   - Expanded for Departmental needs, for example Social Care and Education;
   - Apply to all Departmental employees.

4. *The Use of Computers and the Law*
   - A booklet aimed at new starters, forming part of their basic induction training.

This was an impressive example of how policy-making had been tailored to the needs of the all employees and Departments in the organisation. Data protection was included as one of the 10 'Key controls' in the overarching *Information Security Policy*, under the heading 'Data protection legislation must be obeyed'.

Additionally, it demonstrated how data protection considerations were one of many concerning IT security, included in the *Manual* under a section concerning compliance with legal requirements. However, data protection considerations permeated other sections in the *Manual* such as 'Physical and Environmental Security', 'Access Control', and 'Monitoring System Access and Use'. Finally, this organisation had a dedicated Data Protection Group producing various *Supplementary Guidance* and *Departmental Information Security Guidelines* for departments such as Social Care, which "is workable because they have a different set of problems and circumstances than anybody else."

A final example of detailed policy came from a large metropolitan council. This organisation was slightly unusual in that prior to September 2001, the council did not have a corporate policy concerning data protection. Nevertheless, in the six months prior to interview (March 2002), the Council had drafted a *Statement of data protection policy* – a general statement of intention about two sides of A4 in length. The *Statement* specifies the Council's commitment to upholding the data protection principles plus its intention to ensure the following:

- There is a nominated person with specific responsibility for data protection;
- All those processing personal data are trained to do so;
- Information is provided so that people can make enquiries about handling personal data;
- The management of personal data is regularly audited.

This list is not exhaustive, but gives an insight into the main features of a typical data protection statement. Supporting this *Statement* were procedures concerning aspects of the DPA 1998 such as subject access requests, accessing third party information and deleting personal data. The procedures, set out in a manual, were similar to those outlined in West Midlands Data Protection Forum *Data Protection Code of Practice*.

However, a few DPOs were keen to state that detailed policies do not determine data protection compliance. To quote a DPO from a unitary authority that *did* have a corporate data protection policy:

> "My view is that policies are not the drivers. You can have as many policies as you like but people don't read them as they don't have time... It's the day to day practical issues in dealing with access to information which keeps data protection in the limelight."

This is a reminder that it is not what is on paper, but what is happening on the ground that is important. In the words of the aforementioned interviewee, DPOs in local authorities ensured compliance by: "constant reminders and getting [...] a high profile". Personal contacts were developed, procedures questioned and the support of senior management – preferably at a Corporate level - was sought. Networking was the key, and many colleagues in local authorities did not mind interference from the DPO - as prior knowledge of data protection was low, and any assistance drafting policies and procedures was largely welcomed.

Only two local authorities had not, at the time of interview, established policies and procedures for data protection. One, a county council, lacked a central policy concerning the DPA 1998, but acknowledged there was a need to show "where we're standing as an organisation". The interviewees perceived the aim of their data protection policy to: "set the standards of the organisation ... and its intentions in terms of compliance with the Act." Overall, it would be a short "one or two page document". At the time of interview, the DPO was "actually working on that".

The second local authority, a London borough - lacking an explicit policy - intended "to comply with the Data Protection Act as [...] with any other legislation". At the time of interview (April 2002), "policy was a bit on the hoof", but recommendations were expected from a strategic review into "communications, information and marketing", due to report in June 2002. This strategic review was looking to: "consolidate the information management role – looking at both DP and FOI – and make recommendations...". At interview, a

Data Protection Working Group had been established to "consider issues as they are raised", for example monitoring in the wake of RIPA 2000. Yet, an overarching policy – setting out intentions and procedures for dealing with data protection issues on a daily basis - was clearly absent.

*Universities*

Policy-making at the universities interviewed was impressive, especially given the resource constraints discussed in section 7.2. This was largely due to the persistence of the DPOs interviewed. Two universities had published detailed *Data Protection Handbooks*, both of which included the institution's data protection policy. The policies differed slightly. The basic aim of the policy of one university, in the words of the DPO, "to inform":

> "It's informing the staff and the students, and any other data subject, of what we're doing with the data; and how they can gain access to it; and giving some guidance as well to academic staff, especially, with things like examination marks etc."

Essentially, the policy is an introduction to the scope and provisions of the DPA 1998, and how they impact on the university. It concludes with the contact details of the DPO. It extends beyond a short statement of intention regarding compliance with the DPA 1998, without being over-long. This statement was devised by the University's Data Protection Working Group, although the onus was on the DPO to update it yearly as she saw fit.

The aim of the second university's policy was to state its intention to comply with the DPA 1998. Further, the policy stated that the university:

> "will seek to ensure that the rights of all data subjects for which it has responsibility are observed and that *these rights are made explicit.*" [Author's emphasis]

This was in contrast to a few of the Councils interviewed, whose DPOs expressed reluctance at publicising data subject access rights was discussed in section 7.3. The third and final paragraph of the policy statement outlined the responsibilities within the university hierarchy for ensuring compliance with the legislation. The scope and provisions of the DPA 1998 are dealt with in a separate section of the *Handbook.* Thus, two institutions in the same sector had differing but equally effective policy statements. As with the previous university, this institution's statement and *Handbook* were devised by the DPO. Other departments in that university were consulted when the policy was drafted, and a Data Protection Working Group had been established but "meetings were difficult" as data protection had not been viewed as a priority.

The *Handbooks* of both universities were comprehensive, covering both generic issues - such as SARs and archiving - and education-orientated concerns, for example, examination marks, references and research data. In the *Handbook* of the second institution, additional consideration was given to student debt, CCTV and storage media, and careers and counselling services. Both publications had appendices attached, concerning model application forms for SARs, and in the case of the latter university, notice of student debts held and notice of staff data held. In contrasting ways, both *Handbooks* represent model guidance for higher education institutions.

The policy of the final university was a little more basic. The institution had recently drafted a new policy, although an older version was displayed on its website. The new policy was:

> "...just a brief thing – minimal compliance: "We will do what we need to do; we have a DPO", and that's about it really."

Staff attention had been drawn to it via circulars, and it was intended to be posted on the university website for wider coverage. It, too, was developed by the DPO in consultation with a Data Protection Working Group. However, at the time of interview, interest in data protection had "fizzled out", and the Working Group had not met for over 18 months.

*Other case study organisations*

In the remaining case study organisations, progress had been mixed. The health authority did not have a policy but were "hoping to develop one". The DPO was fully aware of the need for a general policy for data protection, and another policy concerning information security – hugely important in an organisation processing sensitive patient data. At the time of interview (April 2002), the DPO was seeking advice on how to draft such a policy, which would be written by the DPO and commented on by the authority's Data Protection Working Group and departments.

The police authority did have a data protection policy in the Force's *Data Protection Manual* contained the *Manual's* two generic chapters. However, the DPO was moving towards a code of practice approach, with codes for each system. For example, in relation to the CCTV systems this would be a code which:

> "incorporates the Police and Criminal Evidence Act requirements, data protection requirements, police covert surveillance requirements, and so on".

In some ways this integrated approach, putting the systems first mirrored the 'information security' approach of the county council highlighted in earlier in this section. In the police authority, the onus in producing the codes of practice was placed on those working at the front-line. This was done for two reasons. Firstly, those people would have the most intimate knowledge of the system. This would allow the DPO to deliberately relegate himself to a consultancy role. Secondly, it would ensure a more pro-active approach to data protection by those who actually used the systems:

> "That's been successful, because the codes of practice when they've eventually been completed – and it's a matter of hand-holding, and giving them some models – they've been quite good."

Previously, when the DPO had produced guidance and passed it down to the nominated officers: "They had returned it saying: 'Yes, it's OK', whether it was or not". By having actual input into the codes, such officers were forced to be more critical. The police authority did not have a data protection policy group as such, but there was a group of practitioners:

> "...who meet and assist in determining the codes of practice: the operating rules; the issues relating to that system etc. That should feed through to a nominated officer with overall responsibility for the system."

However, the effectiveness of those groups and that structure really depended "on the interest of that nominated officer." Policies are generally reviewed "between two and five years, except for those that are moving quite rapidly at the time". For example, the policy concerning emails had been reviewed three times in the previous six months. Fundamentally, the police authority had an impressive, structured system for policy-making which involved considerable, critical participation by those with the greatest involvement in the systems affected.

Finally, the education organisation had a straightforward policy agreed by its Director-General. The policy – like most in this Chapter - was a statement of intention underpinned by standards, subject to a peer review process every three years. There was not a specific data protection group, but a senior management group – the Electronic Services Committee – that considers data protection as part of its general interest "in the whole of IT".

### 7.6.3 Data protection 'built-in'?

As the analysis in the previous section demonstrates, data protection is increasingly being 'built-in' as part of an organisation's general information strategy. An interviewee at a unitary authority stated that data protection "gets a mention in departmental information strategies", whilst a metropolitan council DPO stated:

> "All Council policies I've been able to get my fingers on have been updated to include standards relating to DP, so staff are aware there are issues."

Such policies included loans, recruitment and selection, housing and social services. Development of data protection as standard procedure was notable in the universities where, in words of one DPO, there had been "considerable progress" with graduation and alumni data. Typical measures included opt-outs from publishing names during graduation and using ID numbers instead of names when displaying graduation data on notice boards. Progress had also been made in publishing email addresses of staff on Internet directories, with an opt-out from the directory being proposed. Areas for further development in one university included the use of sensitive data for research, with progress to be made before all data is anonymised whilst being processed. In the words of a university DPO:

> "Considerable improvements have been made in building-in data protection, but it remains a slow, painful process".

The police authority's code of practice approach was successfully integrating data protection into the Force's many systems, whilst the health authority acknowledged the need for a "proper records management strategy" incorporating the requirements of the DPA 1998, *Caldicott* and information security. Progress had been made in the health authority towards BS 7799 – the standard for information security that several case study organisations were working towards.

Other difficulties mentioned were inserting data protection clauses in contracts with data processors, often conducting specific duties for the organisations. Further problems concerned schools displaying photographs on the internet without permission of the data subject. This could be sensitive if, for example, the child is in hiding from a violent parent. One metropolitan authority interviewed amended its procedures to inform parents when promotional photographs were being taken. This was in order to give them the chance of opting out. Finally, in a London borough a DPO blamed internal politics - "power and control of your own ends in Departments" - for hindering development of an integrated data protection policy. However, change was underway, with the DPO gaining centralised

control of the all Council's forms over the intranet. This will enable the interviewee to "find out all the ones that haven't got the data protection stuff!" As a whole, analysis of the case study interviews suggested that data protection was becoming a standard part of forms, reports and contracts along with financial and environmental concerns. Data protection was thus becoming part of standard procedure.

### 7.6.4 Evaluation

To ensure that data protection policies extend further than statements of intention, rigorous evaluation procedures are vital. In almost two-thirds of the organisations interviewed, some form of monitoring and review process was underway. Auditing - internal and external – proved the common method of measuring compliance. A DPO in a metropolitan council conducted occasional audits of Departments, usually by invitation and just to check, for example, that contact lists are locked away at night. A small district council had been audited for data protection by a private company of accountants – highlighting issues such as having a clear desk policy, established retention periods for data and telephone email and internet usage policies. Another metropolitan council was unique among the case study organisations interviewed, in that they subjected their procedures to a voluntary 'health check' by the District Auditor. This was perceived as an objective way of measuring data protection performance according to specific and detailed criteria, such as the handling of SARs. A score was given to each criterion, resulting in an overall percentage which could be compared with other local authorities. At the time of interview, two such 'health checks' had been conducted – the first in September 2001; the second in February 2002. The interviewee concluded:

> "In nearly, if not all, areas we've above average. We've made significant improvements on where we were in most areas. As a percentage, we went from something like 54% to 73%. We've got all the procedures, the policies and everything else in place."

This appeared to be an objective method of measuring procedures on the ground, which determine the success of compliance. It was perhaps surprising that this form of evaluation was only being applied by one of the 12 local authorities interviewed.

The most advanced organisations reviewed data protection policies at set intervals. In one metropolitan authority, policy was reviewed on an annual basis, "to ensure it meets requirements":

> "It comes down to data protection compliance across the Council. Staff training is a way of ensuring compliance. Monitoring incidents and complaints in relation to data protection, and identifying the issues that come out of those."

In a county council, policy was reviewed by the DPO "continuously, when the need arises", but in any event annually "just to make sure". Furthermore, for any guidance and policies published on the internet, the Council were in the process of constructing their own metadata for all webpages[35]. Included in the metadata was the ownership and the review data, which cannot be set more than one year in advance:

> "All of these things will be published in that way, so that they've got to physically enforce the review date... Those papers will be checked through. They can just be left: "We've reviewed them, we're happy with them, we don't want to make any changes", and put the review date back for another year. Which is OK."

Other organisations were less sophisticated. A few admitted that not enough work had been done to warrant full-scale audits. At the time of interview, one DPO based in a district council stated:

> "I go around with my ears and eyes open, and when I hear or see something I'm not comfortable with, I try to act on it."

At a unitary authority the DPO sent out constant reminders and ensured the post was given a high profile. An interviewee in a university was more damning. Although an audit was in progress, it had been delayed by a year and there was still "a need for a database of the records they possessed and where they were being held".

In most case study organisations, evaluation of data protection compliance at some level was becoming routine. The majority of organisations interviewed had a Data Protection Working Party or Steering Group comprised of the DPO and Departmental DPRs to monitor compliance. In the words of a DPO at a metropolitan council, compliance included "identifying staff training needs, drafting policies and allocating responsibilities for audits". In this respect, compliance was being ensured in the majority of the organisations participating in the case studies.

## 7.7 Conclusions

The complexities of the issues surrounding the DPA 1998, and its wide application to almost all information processed by public authorities, ensures that compliance is not going to be an easy task. Nevertheless, when measured against the criteria outlined in this Chapter, some organisations were close to achieving full compliance. The key to observance lay in a full-scale review of organisational records management practices. In order for such a review to be successful, the nominated individual responsible for data protection – the DPO – required the full support of the organisation's executive. Status and influence were crucial to the task of implementing the change to data handling practices, essential to ensure full compliance. In the health authority, and the small district councils, this had not been forthcoming. Thus, in spite of the best intentions of the DPOs in those organisations, progress was slow. Moreover, the DPO needed to be situated in 'Corporate Services' or the equivalent. Although a DPO did argue convincingly for a position in Finance department, data protection needed to be a central post with access to the executive and the key policy-makers in the organisation.

Moreover, the nature of the post was changing. In many organisations, it was becoming more a general records management post of the type recommended in the Performance and Innovation Unit's *Privacy and data-sharing* report published in April 2002:

> 'Public service bodies should consider [...] the appointment of a board level Chief Knowledge Officer as a means to ensure integration of information issues into decision-making processes.'[36]

This role combines a range of functions including: data protection and freedom of information; electronic records and document management; and ICT systems and services. It has the advantage of lending a more integrated approach to information management, with data protection and freedom of information concerns being incorporated 'into mainstream decision-making processes' such as business design[37]. Although not a suitable model for all the organisations studied in this Chapter, there were signs that this approach is developing in the county council and police authority in particular.

A crucial part of the role of the DPO was to train staff and promote awareness of the Act. It was disappointing to note that a minority of interviewees did not perceive their role as raising awareness of individual rights outside of their organisation. This attitude appeared at odds with the professed public service ethos of their organisations. Moreover, it appeared myopic, as it denied authorities through the processing of SARs, the most practical test of how their systems complied with the Act. Staff training, however, was well planned and documented. At a basic level, all but one of the case study organisations had delivered presentations concerning the DPA 1998. Most used the intranet as a tool for providing further information on the Act, and saw the need for data protection training to form part of the induction – although, in practice, many organisations failed to train new starters in data protection. This situation needed to be addressed. Additionally, training needed to be more targeted to the requirements of the individual employees. In a large metropolitan council, the data protection training requirements of a caterer differed greatly from those of an IT analyst.

The procedures in place for handling SARs – perhaps the greatest test of data protection compliance - were impressive. Clearly, the majority of DPOs had researched the issue thoroughly, and most had published policies and model forms for handling data subject requests for personal data. However, the small number of corporate – as opposed to departmental requests – received by organisations was surprising. The low volume perhaps indicated a lack of awareness among data subjects of their rights – a factor that case study organisations, as well as the OIC, could contribute to improving. Finally, only a few case study organisations had introduced centralised documenting procedures. This is recommended by the author for all organisations, and has the following advantages:

- It will test the workability of SAR procedures ensuring deadlines are met and the data subject receives a professional service;
- It will enable the DPO to demonstrate compliance with any internal performance indicators;
- It will provide evidence of action on part of the organisation, should any SARs result in litigation.

Finally, written policies and procedures were in place in most case study organisations. In order to satisfy any potential audit by the OIC, the author believes it is advisable that organisations have both:

1. *A short statement of intention to comply with the DPA 1998.*

This would emphasise the organisation's intention to ensure the rights of all data subjects for which it had responsibility were observed and made explicit. It would state the allocation of responsibilities for ensuring data protection compliance and conclude with contact details of the organisational DPO. The full statement need not exceed one side of A4. The statement frequently made the following assurances:

(i) That there is a nominated person with specific responsibility for data protection;

(ii) That contact details are provided so data subjects can make enquiries about handling personal data;

(iii) That opinions are carefully and professionally expressed;

(iv) [*If relevant*] That the organisation reserves the right to charge for access to personal data;

(v) That data sharing with external agencies will be the subject of a written agreement setting out the powers that permit the exercise, together with its scope and controls;

(vi) That all those processing personal data on behalf of the organisation will be trained to do so;

(vii) That the management of personal data is regularly audited.

The above list is not exhaustive. However, it has been drawn from the policy statements of various case study organisations interviewed, representing a solid outline of what should be included in a basic policy document. The majority of organisations had published such documents, which tended to be revised annually. Such reviews highlighted incidents and complaints in relation to data protection, identifying any issues that arose and needed to be fed back into the policy.

2. *Detailed procedures on how to achieve data protection compliance.*

The procedures can take various forms. Some organisations had a single, bound *Handbook* or *Code of practice*. These were aimed at all employees in the organisation, and could be supplemented by more detailed guidance for managers and practitioners in certain departments. Other had separate *Codes of practice* or *Supplementary guidance*, taking the form of specialist papers published where specific issues required additional guidance. These were intended for IT practitioners and management, with a generic introduction to the DPA 1998 – perhaps in booklet form – for the remainder of employees.

The experience of the five West Midlands metropolitan councils in drafting and implementing their *Data Protection Code of Practice* prove that good practice procedures can be shared across similar organisations. It was significant that DPOs in other authorities outside of the region had referred to members of the

West Midlands group for data protection policy advice. This author recommends that networking is further encouraged across all local authorities, and in other sectors such as higher education – where two universities had produced remarkably similar *Data Protection Handbooks* – health, and the police.

Generally, policy-making involving data protection had taken two approaches:

(i) *Data protection-centric*

In the majority of case study organisations, policy had - first and foremost – been orientated around data protection. Specific policies had been drafted with data protection at their heart. These policies only applied to information covered by the DPA 1998 and relevant legislation that impacts upon it. Data protection was being built into departmental strategies, but this was often by insertion of a specific clause, rather than full integration from the outset.

(ii) *Integrated information strategy*

This had been the general approach of a minority of case study organisations, for example a county council and the police authority. In both organisations, data protection was given considerable importance. However, from the outset, it was viewed as just one pillar of a more general information strategy. In the county council, data protection formed part of the *Information security policy*, with data protection concerns permeating all considerations in this policy, including 'Physical and environmental security' and 'Access control'. In the police authority, this was reflected by the DPO's code of practice approach, tailoring codes that included data protection around the needs of the various police force systems.

A few case study organisations fell halfway between the two approaches. The recommendations in Chapter 8 outline how data protection policy can be developed in public organisations, building on the findings of this thesis. For

successful compliance, data protection considerations must become part of standard procedure, built-in to organisational strategies in the same way financial, environmental and personnel considerations have been. If this is achieved, then data protection should not be an issue that requires continual promotion and high profile.

---

**References and Notes**

[1] Unitary authorities were formed in England between 1995 and 1998. They perform a combined role of 'first-tier' county councils and 'second tier' borough, or district, councils.

[2] Relating to cities and some other urbanised districts.

[3] A computerised system, part of the Information Management and Technology (IM&T) Strategy - the NHS strategy to support the sharing of all types of information subject to security and confidentiality safeguards.

[4] For example, refer:

- Great Britain. Office of the Information Commissioner. *The Employment Practices Data Protection Code - Part I: Recruitment and Selection.* Wilmslow, 2002.

[5] Great Britain. Cabinet Office. Performance and Innovation Unit. *Privacy and data-sharing: the way forward for public services*, 2002, p. 122

[6] For further details, refer: http://www.bcs.org/iseb/ [Accessed 16/01/03].

[7] Responsible for implementation of recommendations of the Caldicott Committee. The Committee was commissioned by the Chief Medical Officer of England due to increased concern about the manner in which NHS patient information was being used in England and Wales. It reported in December 1997, presenting 16 recommendations relating to the handling of patient-identifiable information, including the appointment of a senior person in each health organisation to act as 'guardian, responsible for safeguarding the confidentiality of patient information'. In theory, each dataflow was to be tested against six principles of good practice. For further details:

- Great Britain. Department of Health. *The Caldicott Committee: Report on the review of patient-identifiable information*, 1997. URL: http://www.doh.gov.uk/confiden/crep.htm [Accessed 16/01/03].

[8] Question 2 of the survey asked about compliance measures. Out of the 107 who replied, 85 (79.4%) trained in-house, and less than one third (33, 30.8%) of organisations had used external trainers

[9] This short video concerned data protection compliance (or lack of it) in a small office environment. It can be obtained by contacting the OIC. For details, refer: http://www.dataprotection.gov.uk/ [Accessed 16/01/03].

[10] The *Local Government Act 1989* was amended in late December 1999 to replace compulsory competitive tendering (CCT) for local government with the Best Value Principles. The *Local Government Act 1989* (as amended) sets out the six principles that councils must observe.

[11] For education and medical records, organisations can charge more (up to £50). Refer:

- Great Britain. Home Office. *The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000*, No. 191.

[12] This figure came from an interview conducted at a London borough in April 2002.

[13] From an interview conducted with a metropolitan council in March 2002.

[14] The Criminal Records Bureau (CRB) was established as the new agency to conduct checks on convictions histories for employers. This work had previously been done by local police forces. The changeover occurred in March 2002, but at the time of interview in April 2002 this process was far from complete. For further information, refer to the CRB website: http://www.crb.gov.uk/ [Accessed 16/01/03].

[15] Great Britain. Office of the Information Commissioner. *Data Protection Act 1998: Legal guidance*, 2001.

[16] This anecdotal evidence stated that whilst Compliance Officers earned approximately £15 000 at the OIC, some had taken up positions with similar responsibilities in the private sector paying £30-40 000.

[17] This statement was supported by anecdotal evidence during a visit to the OIC in September 2001. Moreover, the Assistant Data Protection Commissioner complained in an aside about staff being "poached" by local government organisations during a conference presentation in May 2001:

- Smith, D. Assistant information Commissioner. The Employee Code of Practice. *Keep IT Legal 4th Annual Conference*, Nottingham. 16 May 2001.

The issues of pay, grading and progression – all long-term concerns of the OIC – were finally beginning to be addressed in February 2002. Refer:

- Great Britain. Office of the Data Protection Commissioner. *Annual Report and Accounts for the year ending 31 March 2002*, 2002, p.9.

[18] Known as the West Midlands Local Authorities Data Protection Forum.

[19] West Midlands Local Authorities Data Protection Forum. *Data Protection Code of Practice*, 2001.

[20] Refer, URL: http://www.socitm.gov.uk/ [Accessed 16/01/03].

[21] For IDeA data protection downloads, refer: http://www.idea-infoage.gov.uk/services/dp/download/ [Accessed 16/01/03].

[22] University of Hull. Information Law and Technology Unit. *JISC Data Protection Code of Practice for the HE and FE Sectors*. Version 2.0, 2000. Refer: URL: http://www.jisc.ac.uk/pub00/dp_code.html [Accessed 16/01/03].

[23] Its members are police officers who hold the rank of Chief Constable, Deputy Chief Constable or Assistant Chief Constable, or their equivalents, in the 44 forces of England, Wales and Northern Ireland, national police agencies and certain other forces in the UK and Channel Islands, and senior civilians. There are presently 280 members of ACPO. Refer: http://www.acpo.police.uk/ [Accessed 16/01/03].

[24] To view a copy, refer: http://www.cyber-rights.org/documents/acpo_data_protection_code.htm [Accessed 16/01/03].

[25] *BSI-DISC Guides to the Data Protection Act 1998* (PD0012). Refer: http://www.bsi-global.com/Portfolio+of+Products+and+Services/Books+Guides/Data+Protection/index.xalter [Accessed 16/01/03].

[26] This Guide was originally produced in 1998 by Oppenheim and Davies at Loughborough University:

- Oppenheim, C. and J.E. Davies. *Guide to the practical implementation of the Data Protection Act 1998.* London: BSI, 1998.

It was revised in 2000. Refer *ibid.*

[27] *BSI-DISC Guides to the Data Protection Act 1998*, ref. 25.

[28] Refer URL: http://www.ncc.co.uk [Accessed 16/01/03].

[29] To search NCC guides, refer URL: http://www.ncc.co.uk/ncc/guides.cfm [Accessed 16/01/03].

[30] Chalton, S. et al. *Encyclopedia of data protection*, 1988.

[31] Refer URL: http://www.masons.com/ [Accessed 16/01/03].

[32] Refer URL: http://www.twobirds.com/ [Accessed 16/01/03].

[33] 'The Council' is the generic term referring to the five councils that created and adopted the *Code of Practice.*

[34] West Midlands Data Protection Forum. *Data Protection Code of Practice*, ref. 19, p.16.

[35] Simply 'data about data', metadata comprises structured data about digital (and non-digital) resources that can be used to help support a wide range of operations. At a web-level, metadata facilitates both the management and processing of webpages. Moreover, such data enables users to discover resources (for example, searching the web to find resources on data protection policy).

[36] Performance and Innovation Unit. *Privacy and data-sharing*, ref. 5, p.124.

[37] *Ibid.*, pp.91-4.

# 8. Conclusions and recommendations

This final Chapter will consider the original aim of this thesis. By testing the hypotheses and objectives set out in Chapter 1, this Chapter will evaluate the extent to which the aim has been achieved - and indicate where further research can be conducted. Firstly, an outline of the thesis is provided. Following this, hypotheses 1 and 2 are considered, with an assessment being made of the extent to which the objectives of each have been fulfilled. Additionally, findings from both desk research and fieldwork are considered. Finally, recommendations are made: firstly, to stakeholders concerning the further policy development; and secondly, for further academic research.

## 8.1 Outline of thesis: aim and hypotheses

The overall aim of this thesis was:

> **To investigate and analyse the extent to which public organisations have achieved compliance with the Data Protection Act (DPA) 1998.**

In order to achieve this aim, two hypotheses were tested. The primary hypothesis, directly addressing the aim, stated:

> **1. At an organisational level, the DPA 1998 represents a positive measure for ensuring compliance and good practice.**

The secondary, broader, hypothesis set the DPA 1998 in context with previous UK data protection legislation, and similar legislation abroad. Additionally, it sought to understand the regulatory framework, and the extent to which it enabled compliance with the DPA 1998. It stated:

**2. The DPA 1998 has built on previous legislation in the UK, and abroad, in order to strengthen the individual right to informational privacy. Within the UK, a regulatory framework has been established, enabling this right to be exercised effectively.**

Finally, a subsidiary hypothesis sought to critically compare provisions of the DPA 1998 and other key UK legislation, drawing out any ambiguities and potential for confusion.

**The DPA 1998 works effectively with other legislation impacting on data protection. Overlap is minimal and meaning is clear.**

This subsidiary hypothesis acknowledged the evolving legislative environment, which in the space of eighteen months witnessed the coming into effect of significant legislation including: Human Rights Act (HRA) 1998; Regulation of Investigatory Powers Act (RIPA) 2000; Freedom of Information Act (FOIA) 2000; and the Anti-Terrorism, Crime and Security Act (ATCSA) 2001.

The hypotheses were tested using a rigorous methodology based on triangulation of research. Lines of enquiry opened up through desk research were backed up by fieldwork. The desk research – supported by expert interviews - afforded a wide appreciation of the key data protection issues facing organisations. A questionnaire survey provided a gateway for the case studies – permitting an insight into the data protection issues facing organisations on a daily basis. The case studies expanded the survey's findings, focusing on the detailed policy-making processes affecting the protection of personal data. In short, the methodology established an evaluative framework – assessing the strengths and weaknesses of internal data protection policies in order to assist public organisations in their policy-making and legislative compliance.

## 8.2 Hypothesis 1: compliance and good practice

**At an organisational level, the DPA 1998 represents a positive measure for ensuring compliance and good data handling practice.**

This hypothesis was addressed completely. It can be stated with certainty that the DPA 1998 was perceived as - and in practice represented - a positive measure for compliance and good data handling practice. The effect of FOIA 2000 in particular, due to be enacted in 2005, was seen as a boon to the DPA 1998. Furthermore, the objectives, setting out how each Hypothesis was to be investigated, were fulfilled.

*Analysis of objectives*

The questionnaire survey polled attitudes of practitioners concerning the workability of the DPA 1998. Most respondents (75, 70.1%) strongly agreed or agreed that the DPA 1998 is a positive measure for ensuring compliance and good practice. Only 14 respondents (13.1%) disagreed or strongly disagreed with this viewpoint.

The case study interviews, with Data Protection Officers (DPOs) from 18 organisations, helped identify the processes in working towards compliance with the DPA 1998. Whilst no organisation claimed to be fully compliant, the vast majority had made major changes to organisational practices in response to the enactment of the Act. Key modifications included: the increased status of the DPO; development of detailed training plans aimed at staff throughout the organisation; implementation of procedures for the enactment of subject access requests – and the publicising of that right; and the drafting of data protection policies and procedures designed to ensure compliance throughout the organisation. The changes were considered in detail in Chapter 7. Fundamentally, it can be stated that Hypothesis 1 has been proved to be correct.

Recommendations for further best practice – over and above those initiated by most case study organisations – have been given in section 9.4 of this Chapter. In

November 2002, they were presented at the conference of the National Association of Data Protection Officers in Warwick, in order to gain practitioner feedback. The feedback has been taken seriously by this author, and incorporated into Chapters 8 and 9 of this thesis.

## 8.3 Hypothesis 2: privacy and the interface with other key legislation

**The DPA 1998 has built on previous legislation in the UK, and abroad, in order to strengthen the individual right to informational privacy. Within the UK, a regulatory framework has been established, enabling this right to be exercised effectively.**

- **The DPA 1998 works effectively with other legislation impacting on data protection. Overlap is minimal and meaning is clear.**

The secondary hypotheses considered the context to – and the scope of – the DPA 1998. Additional consideration was given to the role of the OIC, especially in promoting codes of practice, and to practitioner views on compliance advice received from the supervisory authority. These hypotheses were more wide-ranging and, consequently, more difficult to quantify. The objectives, largely addressed through desk research and expert interviews, were thus not entirely fulfilled.

*Analysis of objectives*

Firstly, Chapter 4 set the DPA 1998 in context with previous data protection in the UK and abroad. In its 30 year history, data protection law had clearly evolved: from the early national laws in Sweden and Germany reacting largely to domestic concerns about the role of government computers; to international instruments such as the EU Data Protection Directive. The latter specifically mentioned the individual right to privacy, and the need to ensure the free transfer of personal data between EU member states to facilitate the Single Market. In comparison to

national data protection laws within the EU and further afield, the UK DPA 1998 was demonstrated to be pragmatic and flexible. It shunned its human rights origins by not referring to 'privacy' at all. Instead, the complex text set out eight 'principles' that data controllers should follow in order to achieve compliance. A number of practitioners complained that the lack of explicit guidance made the text of the Act "woolly". This increased the pressure on the supervisory authority, the Office of the Information Commissioner (OIC), to develop clear guidance. Additionally, the OIC was granted powers in the new Act to develop codes of practice in order to develop best practice in specific fields.

Secondly, desk research established that academic studies in the field of data protection, commencing in the US in the mid-1960's, had been many and varied. Much research, such as Bennett and Grant (1999), emphasised the significance of explicit policy choice, with organisations needing to build data protection principles into their practices. However, none had considered in detail the implications of the 1998 Act for public organisations in the UK. Clearly, there was a need for such a study, given the large shadow the DPA 1998 cast over all forms of data processing – computerised and manual. Rule's *Private Lives and Public Surveillance* (1973)[1] represented a earlier generation's detailed research into the field, with case studies including three large UK public institutions: the Driver Licencing system; the Criminal Record system; and National Insurance. The methodology of this PhD thesis owed a little to Rule's approach, which this project sought to develop at a micro-level.

Thirdly, in an attempt to quantify Hypothesis 2, the main provisions of the DPA 1998 impacting on individual privacy were considered in Chapter 4 (section 4.6.2). They included: extension of the scope of the Act to include manual processing; the creation of a new category of sensitive personal data; the prohibiting of the transfer of personal data outside the European Economic Area[2] (EEA) unless certain conditions were satisfied; and the creation of significantly more and stronger individual rights. It is the final provision that has the most direct effect on the privacy of individuals. Such rights included not only rights of access to personal data, but also the right to stop such data being processed for

direct marketing, or that would cause damage or distress to the data subject or a third party.

The role of the supervisory authority in promoting compliance was given consideration throughout the thesis. Desk research outlined the general regulatory framework, the codes of practice, and documents giving opinion for and against the instruments. The expert interviews included a visit to the OIC in Wilmslow, in addition to gaining views of others in the field. Finally, questionnaires and case studies elicited comments from practitioners. Naturally, views on the performance of the OIC varied enormously – with business being against any interference in their working practices, trade union representatives in favour of the principles behind the *Employment Practices Data Protection Code*, and practitioners tending to turn to their peers when addressing compliance issues, often finding the OIC's advice slow and contradictory. A number of factors accounting for the views of the practitioners were cited, including the high staff turnover at the OIC, and the excellent levels of cooperation between peer groups – particularly local authority forums such as NADPO and SOCITM.

The final objective in investigating Hypothesis 2 involved critically comparing the provisions of the DPA 1998 and other key legislation already mentioned in this Chapter. Fulfilling this objective proved particularly difficult, given the scope and some of the unknown challenges presented by some of the legislation involved. Certainly, the objective presented manifold options for further detailed research. In summary, considerable legal changes have occurred, nationally and internationally, since the enactment of the DPA 1998. In the UK, the HRA 1998 has resulted in the creation of a common law of privacy for the first time. However, the scope and impact of this statute will take years to assess, as the HRA 1998 has to infiltrate UK case law through the courts. More pertinent to organisations' actual handling of personal and official data are the provisions of FOIA 2000, with its creation of a general right of access to information held by public authorities. At interview, many public authorities were in the process of drafting publication schemes, auditing records and preparing job descriptions for new personnel. The effect of this legislation, due into force in January 2005, will be considerable. Interviewees in case study organisations were fully aware of the

records management significance of such legislation, working as it does in tandem with the DPA 1998.

The impact of other key legislation – such as RIPA 2000 and ATCSA 2001 – on data protection in public organisations was particularly difficult to assess. A satisfactory conclusion has not been reached. RIPA 2000 – aimed at protecting the confidentiality of communications made over a public telecommunications network – created some confusion among employers as to which information organisations could intercept for evidential purposes. The government sought to clarify this issue through the *Lawful Business Practice Regulations*. However, the OIC's release of its *Draft code of practice on employer/employee relationships* in the same month as the government's *Regulations* created confusion about exactly how far employers could go in acquiring employee personal data through monitoring and interception. More than two years later, with the repeated delay of the release of Part 3 of the finalised *Employment Practices Data Protection Code: monitoring and surveillance*, this issue has yet to resolved. When conducting case study interviews (February-May 2002), it was discovered that - for this reason - half the organisations visited had not finalised policies concerning monitoring of employee email and internet usage. Finally, the events of 11th September 2001 compelled many western governments to pass anti-terrorism measures. Of particular relevance to this thesis was Part 11 of the ATCSA 2001, relating to the retention of communications data. Although this is mainly of interest to communications providers such as ISPs, the OIC expressed concern about the basis on which law enforcement bodies could have access to such communications, and the delays in drafting a voluntary code under which such data could be accessed. At the time of writing, the code had yet to be finalised.

In conclusion, to answer the main statement of Hypothesis 2, the DPA 1998 has strengthened the individual right to privacy. This was clear from consulting the text of the legislation - with its increased scope to cover manual records, its creation of sensitive personal data that was afforded greater protection, and in its extended individual rights. Moreover, the role of the supervisory authority has been strengthened – with the OIC able to establish codes of practice and overseeing compliance with the incoming FOIA 2000. The HRA 1998 potentially

strengthens these provisions by enabling courts and tribunals to assess the privacy considerations on a case by case basis, thereby acknowledging the DPA 1998s links to the European Convention of Human Rights, via the EU Data Protection Directive. FOIA 2000 certainly bore out the second statement of this Hypothesis, and has been drafted to 'work effectively' with DPA 1998. In fact, when it comes into force, FOIA 2000 will amend and increase the scope of the Act – allowing data subject access to manually processed data that is 'unstructured'. However, it is clear from desk research – supported by expert and practitioner interviews - that RIPA 2000 and ATCSA 2001 do not 'work effectively' with the DPA 1998, and appear to some extent, to undermine the legislation[3]. Indeed, the provisions of RIPA 2000 and ATCSA 2001 have contributed to a confused regulatory environment that does little to strength the right to privacy.

Suggestions for further academic research addressing the issues raised by Hypothesis 2 have been outlined in the final section of this Chapter.

## 8.4 Recommendations

This thesis has achieved its aim in investigating and analysing the extent to which public organisations achieved compliance with the DPA 1998. Recommendations are now outlined for stakeholders – experts and practitioners - and for further academic research, where safe conclusions have not been reached. The recommendations below build on the findings from the various Chapters of this thesis. Where necessary, they are cross-referenced (quoting the relevant page numbers) for further clarity.

### 8.4.1 Stakeholders

The first two recommendations are aimed at government and the regulatory authority respectively. The remainder are pitched at the DPOs interviewed at case study level. The intention is to build on the findings of the interviews outlined in Chapter 7, and provide hard and fast guidelines of where data protection can

develop. Most of the points below were acknowledged by practitioners themselves as areas requiring further development. In the general course of research the author identified the remainder, with reference being made to the views of the OIC, lawyers, and professional bodies as to what facilitates adequate data protection compliance. Consequently, it is believed that the recommendations for the case study organisations are realistic in terms of financial and human resources involved in their implementation.

*(i) The text of the DPA 1998 to be made more explicit*

This was a clear problem, identified by most interviewees – at expert and case study level. Undoubtedly, the format of DPA 1998 leaves a lot to be desired. On a personal level, research for this thesis would have been more problematic without reference to various newsletters and the JISCmail discussion group to shed light on many topical data protection issues and aid in the interpretation of the case law. It appears strange that the UK DPA 1998 should be so "appallingly drafted" – in the words of one expert interviewee - given that the Directive it enacts is a relatively straightforward and readable piece of legislation. Reference to other contemporary national data protection laws – such as those of Sweden[4] and Canada[5] – demonstrate that concise, clearly drafted statutes in this field are possible. The Data Protection Directive is currently being reviewed by the European Commission, and the UK government has recommended changes to the text of the Act[6].

*(ii) Greater education concerning the DPA 1998*

This recommendation is aimed at the UK's supervisory body, the OIC. Whilst the burden of their work was appreciated, it was widely believed at interview level that more could be done to promote the Act – in particular, data subject access rights. Additionally, the presentation of their material was criticised – especially with respect to *Draft Code of Practice: The use of personal data in employer/employee relationships*, and the confused design of the OIC website. Suggestions for further development include:

- A better-designed and regularly updated website, outlining the latest publications and activities of the OIC. This concern was outlined in response to the questionnaire survey (Chapter 6, section 6.2.1, pp. 272-3);
- Greater consultation on codes of practice from the outset: the CBI in particular complained about not being involved in the production of the *Draft Code of Practice: The use of personal data in employer/employee relationships*. This point was made forcibly by a CBI speaker at a conference on data protection in the employment context[7];
- Greater availability and faster response times of OIC Compliance Officers to reduce delays of up to three months experienced when replying to questions from DPOs. It is appreciated that this recommendation has some resource implications. Complaints about the speed, quality and consistency of advice received from the OIC were made during the questionnaire survey (Chapter 6, section 6.2.1, pp. 272-3), and case study interviews (for example, Chapter 7, section 7.6.1, pp. 317-8);
- Facilitating greater cooperation between public bodies from different sectors (whilst networking among local authorities was excellent, it was singularly lacking among health trusts and between police authorities). The issue of networking, and the role the OIC could play in this, was raised by interviewees in Chapter 7 (Section 7.6.1, pp. 319-321).

With the exception of the issue relating to Compliance Officers, the above recommendations do not pose any great strain on resources, instead involving changes in procedures. Moreover, successful implementation of the above would ensure that DPOs used the OIC more often than perhaps they did at the time of interview, thus enhancing the OIC's status and influence.

*(iii) In order to achieve compliance, organisations need to firstly follow certain basic steps.*

The steps outlined below represent the conclusions to Chapter 7, following interviews with DPOs. Additionally, they build on the compliance criteria established in Chapter 7 (section 7.1.2, pp. 287-90). The list is not exhaustive, nor

will following it guarantee absolute data protection compliance. However, they represent the first moves towards achieving that goal.

- Appoint a *nominated individual responsible for data protection* of sufficient status and influence to fully review organisational records management practices.

  Most organisations had a nominated individual, although the status accorded to the post was sometimes low (section 7.2, pp. 291, 297-8). Admittedly, a fresh appointment would cost additional money, but with the sensitive nature of the records involved and the increased profile that FOIA 2000 gave to records management generally, organisations were beginning to realise that they could not afford to under-fund this area. To quote a DPO in a district council: "you would not want to be the subject of case law".

- *Promote awareness of the DPA 1998 among data subjects* who regularly contact the organisation, for example, local authority council tax payers, university students, and National Health Service (NHS) patients.

  This need not be expensive or time-consuming – it could involve just placing leaflets in public offices. However, the posting of a *Fair Processing Code* (modelled on the OIC's legal advice[8]) on the corporate internet site would highlight how the organisation should obtain information from the data subject, how it will be used and the rights of the data subject to access, correct and delete their personal data. This would help develop trust between case study organisations and the population they serve. This point is made in Chapter 7 (section 7.3, pp. 299-300).

- Devise a *structured training programme tailored to the needs of particular staff.*

  Data protection training needs to be embedded into the organisational structure from the bottom up. Additionally, it should 'relevant to each group' – the requirements of someone working in a local authority Social Services

department differ from a colleague based in Housing. Training strategy has to take account of this. Finally, data protection training needs to become part of the induction process – ensuring that new starters are confident of the issues surrounding the handling of personal data from their first day of employment. A comprehensive strategy should be devised by the practitioner, and approved at board level. There may be some initial expense involved in drafting the programme and in terms of staff time, but savings would be made through better records management and compliance with the DPA 1998, reducing the likelihood of legal action. Examples of training strategies include the targeted training employed by the metropolitan authority outlined in section 7.4.2, pp. 304-5.

- Devise procedures governing the *handling of subject access requests (SARs).*

  Such procedures need to be carefully documented, enabling organisations to monitor the progress of SARs – ensuring deadlines are met and that the data subject receives a professional service (refer to section 7.7, p. 336). Further, the new procedures will enable the postholder to demonstrate compliance with internal performance indicators, and provide evidence of action on part of the organisation should any SARs result in litigation. This recommendation is merely procedural, and should not significantly add to costs.

- Formulate a written *data protection policy*, stating intention to comply, and *detailed procedures*, outlining how data protection compliance is to be achieved.

  These documents would enable procedures to be implemented uniformly throughout the organisation, in addition to providing evidence of compliance in the event of any audit or legal dispute. Well-drafted policies would provide a roadmap for achieving data protection compliance, being flexible enough to incorporate changes in legislation and guidance from government and the supervisory authority respectively. Ideally, data protection concerns should not be considered in isolation, but form part of general "information strategies" (Chapter 7, section 7.6.3, pp. 330-2).

- *Regularly audit data protection compliance.*

Vital if organisations are going to test the effectiveness of their procedures. This can be achieved either internally or externally. Internal audits by the DPO are a good way of quickly checking that procedures are being adhered to – for example, that desks are cleared at night, passwords are not shared, and that lists of contact numbers are not left on general display. An external audit would be an objective measure of these procedures, gaining an additional perspective from the outside. An example would be the voluntary 'health check' by the District Auditor in which one county council participated (section 7.6.4, pp. 332-3). This was more structured, with each compliance criteria being given a score by the District Auditor, resulting in an overall percentage, which could be compared with other local authorities. This may be suited to the larger public authorities. Another external audit option would be to recruit a consultancy group to verify procedures, although this can be prohibitively expensive for many public organisations.

Whatever methods are chosen, it is important that policies and procedures are evaluated on a regular basis. This would be at least once a year, and more frequently where there have been changes to official guidance (for example, monitoring of email and internet usage) or to the law (for example, concerning selling personal data on the electoral roll).

Case study analysis demonstrated that most organisations at least some of the basic recommendations listed above. The areas where compliance was found to be most wanting – documentation of SARs and regularly auditing – could be implemented incurring little additional financial cost. SARs could be recorded using a straightforward database, whilst templates for auditing compliance internally could be acquired from peers, through forums such as the JISCmail data protection discussion list or from contacting professional organisations such as NADPO and SOCITM.

*(iv) Further recommended steps towards compliance.*

The recommendations below build on the basic steps outline in part (iii) above. They have been devised following the author's interviews with case study organisations and study of their procedures.

- Creation of an *integrated records management post*, incorporating the additional workload generated by FOIA 2000.

Based on recommendation 7 in the *Privacy and data-sharing* report (quoted in Chapter 7, section 7.1.2, pp. 287-8)[9]. This would be at senior management level, but - in addition to data protection - this role would comprise freedom of information and human rights. The postholder would therefore be responsible for handling all information, resulting in a more integrated information policy. The post needs to be central with access to the executive and the key policy-makers in the organisation. In the larger organisations interviewed – the police authority, health authority and some metropolitan councils – this new position should be supported by a board level Chief Knowledge Officer, lending the new postholder further authority. Whilst the establishment of the post would cost money, it should generate savings in greater efficiency with which records are managed throughout their life cycle.

- Training the DPO in *Information Systems Examination Board (ISEB) certificate.*

A basic and practical introduction to data protection. As an industry-recognised qualification, would enhance the DPO's status in their organisation. Approximately one third of the interviewees had trained, or were in the process of training, for the certificate (Chapter 7, section 7.2.1, pp. 293-4). However, the costs of upwards of £2 200[10] involved in training with an accredited provider may put this out of reach of the smaller organisations interviewed.

- Developing *policies concerning employee use of email and internet.*

  With well-publicised cases of organisations being sued for damages or employees being dismissed, there is an essential need for clear policies in this field. This is something that organisations can achieve at minimal expense through greater networking – finding policy that best suits their circumstances.

- Improving *information security: aim to be BS 7799 compliant.*

  A requirement of the Seventh Data Protection Principle, BS 7799 is a comprehensive standard that could be used as the basis for data protection policy development. The aim is to be complaint with BS 7799, rather than invest in the actual certificate which one metropolitan authority DPO complained was "very expensive!"[11]

- *Greater networking among organisations.*

  Where good practice exists, it should be shared among similar organisations. Evidence suggested this was occurring between many of the local authorities interviewed (Chapter 7, section 7.6.1, pp. 319-320). However, there was little indication of health authorities sharing practices, accounting for the feelings of isolation experienced by the DPO interviewed. Such networking needs to be encouraged by all professional bodies, whether or not they specialise in data protection. The work of JISC for higher and further education, SOCITM for ICT, and Association of Chief Police Officers all demonstrate that this can happen. The benefits for organisations include: reduction of costs in terms of finance and time, especially in terms of policy-making; exchange of ideas and pooling of resources (for example, establishing which training methods were the most beneficial); and promotion of a sense of community among practitioners, reducing feelings of isolation. The experience of the West Midlands local authorities testifies to the success of such networking.

The stakeholder recommendations listed in this subsection demonstrate how organisations can take data protection forward. They are of relevance to all organisations interviewed, although the size and nature of each body must be taken into account when following the above advice. However, the author believes that consultation with the case study organisations added value to the recommendations outlined in this thesis, lending them a *de facto* practitioner approval[12]. Adherence to the above recommendations should ensure that stakeholders are well equipped to achieve compliance with the DPA 1998.

### 8.4.2 Further research

Data protection is a broad field, opening up many opportunities for further research. The full extent of the research possibilities became apparent when testing Hypothesis 2. The following comprise a few suggestions:

*(i) Data protection in the EU and the US: a comparison*

Two different regimes: historically, legally and culturally. Chapter 4 (section 4.7.1, pp. 152-7) demonstrated the different, self-regulatory, approach taken by the US. Research can involve case studies of organisations on both sides of the Atlantic – comparing data handling techniques, and data subject rights, between the regulatory EU and the self-regulatory US. The impact of the 'Safe Harbor' principles on the practices of US companies can be investigated, assessing whether the commitment of US organisations to the agreement had improved since the mixed findings of the European Commission working paper of 2002[13].

*(ii) Data protection and the HRA 1998*

Although the Data Protection Directive refers to the European Convention on Human Rights, from which the HRA 1998 derived, the link between data protection and human rights remains under-explored. One of the reasons for this is that the amount of relevant case law at the moment is too small to make a

meaningful assessment (Chapter 5, section 5.6, p. 224). However as court cases accumulate over the coming years, such a study could demonstrate why data protection, as opposed to other forms of privacy[14], is a human right. Case studies may involve individuals or organisations that have been significantly affected by such human rights and data protection case law.

### *(iii) Data protection and freedom of information in public organisations*

FOIA 2000 was identified by many experts (Chapter 6, section 6.1.8, p. 258) and practitioners (Chapter 7, section 7.2, pp. 291-2) as the most important future issue regarding their work. Certainly, FOIA 2000 will have a significant impact on the handling of public records when it enters into force in January 2005. This would make a fascinating PhD project, developing the findings of this thesis by studying the interface between the two Acts in similar organisations. Particular attention could be drawn to changes in job descriptions of practitioners, development of publication schemes, staff training, policy development and so on. The categories for data protection compliance outlined in Chapter 7 (section 7.1.2, pp. 287-90) could make a useful starting point.

### *(iv) Data protection and e-government*

How does data protection affect the government's e-government agenda? In April 2002, the Performance and Innovation Unit published the significant report *Privacy and data-sharing*[15] concerning data protection and the efficient delivery of public services. Are the two concerns compatible? The interview with the Office of the e-Envoy in Chapter 6 (section 6.1.4, pp. 249-50) highlighted the tension between the government's obligations under the DPA 1998 and HRA 1998, and their drive to coordinate and integrate public services. Interviews with public authorities in Chapter 7 (section 7.2) developed this issue, with many interviewees being assessed on their e-government targets rather than actual data protection compliance. This is an issue of considerable public policy interest, with the government drafting a 'Public Services Trust Charter' in order to allay public concern about their handling of personal data. Case studies may include the Office of the e-Envoy, charged with delivering the government's e-agenda until

2005, and public organisations from different sectors, as they attempt to deliver more services electronically.

*(v) Data protection and the private sector*

Assess the challenges the DPA 1998 presents to the commercial world. Due to the necessary need to set limits, private sector concerns were omitted from the remit of this thesis. However, a study of data protection compliance in this field would be useful, particularly as an increasing amount of individual data is transferred globally between multi-national companies. Moreover, it would be interesting to assess how the DPA 1998 is perceived by those working in such organisations. Whilst the Act's provisions concerning security of information – in particular Principle 7 – may be welcomed by business as enhancing client trust, improved individual rights to access, correction, deletion and compensation for damage and/or distress could be perceived as increasing costs, and impacting on often tight profit margins. Case studies involving various sectors (for example, retail, financial services, direct marketing) could assess whether the DPA 1998 is viewed as a measure improving good practice or as an additional burden on business.

## References and Notes

[1] Rule, J.B. *Private lives and public surveillance.* London: Allen Lane, 1973.

[2] The European Economic Area is the fifteen EU member states plus Iceland, Liechtenstein, and Norway.

[3] Refer to Chapter 5 (section 5.5) for a more detailed discussion of the complexities brought about by RIPA 2000 and ATCSA 2001.

[4] Sweden. *Personal Data Act 1998*, Swedish Code of Statutes, SFS 1998: 204.

The Personal Data Act has 51 sections, all clearly headed. The Act commences with definitions, including 'consent', and concludes with details about transitional provisions. The processing requirements for both sensitive and non-sensitive personal data, and transfers of data to third countries, are explained *within* the Act.

[5] Canada. *Personal Information Protection and Electronic Documents Act*. (2000, c.5). URL: http://laws.justice.gc.ca/en/P-8.6/ [Accessed 16/01/03].

The structure of this Act is not dissimilar to Sweden's Personal Data Act, commencing with a summary of its provisions, followed by definitions and concluding with 10 data protection principles as set out by the Canadian Standards Association.

[6] Refer:

- Great Britain. Lord Chancellor's Department. Data Protection Directive – European Commission's Report on Implementation. *United Kingdom response to Commission questionnaire*, 2002.
  URL: http://www.lcd.gov.uk/ccpd/saguide.htm [Accessed 16/01/03].

- Great Britain. Lord Chancellor's Department. Data Protection Directive (95/46/EC). *Proposals for amendment made by Austria, Finland, Sweden and the United Kingdom. Explanatory note*, 2002.

[7] Armitage, R. Head of Legal Affairs, CBI. The business perspective. *Keep IT Legal 4th Annual Conference*, Nottingham. 16 May 2001.

[8] Great Britain. Office of the Information Commissioner. *Data Protection Act 1998: Legal guidance*, 2001, pp. 30-5.

[9] 'All public sector organisations should have a named senior manager with clear responsibility for the handling of personal information'.

Refer: Great Britain. Cabinet Office. Performance and Innovation Unit. *Privacy and data-sharing: the way forward for public services*, 2002, p. 122

[10] This figure was gained via a telephone conversation with an accredited training provider, and did not include VAT, nor the £132 examination fee.

[11] A telephone conversation with BSI Management Systems revealed that application for the standard would cost £512 and an on-site assessment would cost £780 per day. The period of assessment would vary depending on the size of the organisation. For further details of the processes involved in registration, refer URL: http://emea.bsi-global.com/InformationSecurity/ISMSregistration/BSIRoutetoReg.xalter [Accessed 23/05/03].

[12] The recommendations were presented by the author to NADPO members at their annual conference in November 2002. Refer:

- Warren, A. Data protection in public organisations. *NADPO annual conference*, University of Warwick, 18-19 November 2002.

[13] European Communities. Commission. *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*. Brussels, 13/02/02. SEC (2002) 196. URL: http://europa.eu.int/comm/internal_market/en/dataprot/news/index.htm [Accessed 16/01/03].

[14] Privacy International refer to four aspects of privacy:

- Information privacy (also known as 'data protection');
- Bodily privacy;
- Privacy of communications;
- Territorial privacy.

Refer: Privacy International and EPIC. *Privacy and Human Rights 2002*, 2002. URL: http://www.privacy.org/pi/survey/phr2002/ [Accessed 16/01/03].

[15] Performance and Innovation Unit. *Privacy and data-sharing*, ref. 9.

# Bibliography


6, P. *The future of privacy: volumes 1 and 2.* London: DEMOS, 1998.

Aiken, O. Statutes of liberty. *People Management*, 1999, 5 (12), 48-52.

Arthur, C. Now Bush wants to scrap deal on internet privacy. *The Independent*, 31/03/01. (URL: http://www.independent.co.uk) [Accessed 16/01/03].

Bainbridge, D. and G. Pearce. Tilting at windmills – has the new Data Protection law failed to make a significant contribution to rights of privacy? *The Journal of Information, Law and Technology* [online], 2000 (2). (URL: http://elj.warwick.ac.uk/jilt/00-2/bainbridge.html) [Accessed 16/01/03].

Banisar, D. Freedom of information and access to government records around the world. *Privacy International*, 2002. (URL: http://www.freedominfo.org/survey/) [Accessed 16/01/03].

BBC News Online. Forum: Human Rights Act - Quiz Lord Lester. *BBC News Online.* 06/10/00.
(URL:
http://newsvote.bbc.co.uk/low/english/talking_point/forum/newsid_954000/954831.stm) [Accessed 16/01/03].

BBC News Online. 'Kiss and tell' footballer named. *BBC News Online*. 30/03/02. (URL: http://news.bbc.co.uk/1/hi/uk/1901566.stm) [Accessed 16/01/03].

BBC News Online. Blunkett backs ID card plan. *BBC News Online*, 04/07/02. (URL: http://news.bbc.co.uk/1/hi/uk_politics/2084860.stm) [Accessed 16/01/03].

BBC News Online. Mirror wins Campbell appeal. *BBC News Online.* 14/10/02. (URL: http://news.bbc.co.uk/1/hi/uk/2327385.stm) [Accessed 17/01/03].

Bell, J. *Doing your research project.* 3rd edition. Buckingham: Open University Press, 1999.

Bennett, C.J. Regulating the computer: comparing policy instruments in Europe and the US. *European Journal of Political Research*, 1988, 16 (5), 437-466.

Bennett, C.J. *Regulating privacy: data protection and public policy in Europe and the United States.* New York: Cornell University Press, 1992.

Bennett, C.J. Privacy protection in Canada and the US: the implications of September 11th. *Privacy Conference*. Rathenau Institute, The Hague, Netherlands, 17/01/02.

Bennett, C.J. and R. Grant (eds). *Visions of Privacy: policy choices for the digital age.* Toronto: University of Toronto Press, 1999.

Bergfeld, J.P. EC Data Protection Directive, impact on Dutch data protection law. *The Journal of Information, Law and Technology* [online], 1996, 1. URL: http://elj.warwick.ac.uk/jilt/dp/1dutch/default.htm [Accessed 16/01/03].

Best, K. and R. McCusker. The scrutiny of the electronic communications of businesses: striking the balance between the power to intercept and the right to privacy? *Web Journal of Current Legal Issues* [online], 2002 (1). (URL: http://webjcli.ncl.ac.uk/2002/issue1/kb-rm1.html) [Accessed 17/01/03].

Blume, P. The citizens' data protection, *Journal of Information, Law and Technology* [online], 1998, 1. (URL: http://elj.warwick.ac.uk/jilt/infosoc/98_1blum/blume.htm) [Accessed 16/01/03].

Borking, J. and C.D. Raab. Laws, PETs and Other Technologies for Privacy Protection. *The Journal of Information, Law and Technology* [online], 2001, 1. (URL: http://elj.warwick.ac.uk/jilt/01-1/borking.html) [Accessed 17/01/03].

Bourne, C. and J. Benyon (eds). *Data protection: perspectives on information privacy*. Leicester: University of Leicester Continuing Education Unit, 1983.

Burkert, H. Institutions of data protection: an attempt at a functional explanation of European national data protection laws. *Computer Law Journal,* 1982, 3 (2), 167-188.

Burkert, H. Privacy-data protection: a German/European perspective. *Second symposium of the German American Academic Council's Project 'Global Networks and Local Values',* Woods Hole, Massachusetts, 3-5 June 1999 pp.43-69. (URL: http://www.mpp-rdg.mpg.de/woodsh.html) [Accessed 16/01/03].

Burnes, C. Human rights in employment. *Privacy and Data Protection*, 2000, 1 (2), 4-5.

Buxton, R. The Human Rights Act and private law. *The Law Quarterly Review*, 2000, 116, 48-65.

Campaign for Freedom of Information. Deeply disappointing Information Bill 'weaker than Conservatives' openness code'. *Campaign for Freedom of Information*, 24/05/99. (URL: http://www.cfoi.org.uk/draftbill240599pr.html) [Accessed 16/01/03].

Campaign for Freedom of Information. FOI Bill: Lords Third Reading Briefing. *Campaign for Freedom of Information*, 21/11/00. (URL: http://www.cfoi.org.uk/newin00.html) [Accessed 16/01/03].

Campaign for Freedom of Information. Government to abandon freedom of information timetable? *Campaign for Freedom of Information*, 02/11/01. (URL: http://www.cfoi.org.uk/newin01.html) [Accessed 16/01/03].

Campaign for Freedom of Information. *Double blow for FOI*, 13/11/01. *Campaign for Freedom of Information.* (URL: http://www.cfoi.org.uk/newin01.html) [Accessed 16/01/03].

Canada. *Anti-Terrorism Act*. (2001, c.41).

Canada. Department of Communications and Department of Justice. *Privacy and Computers: a report of a Task Force*. Ottawa: Public Works and Government Services Canada - Publishing, 1972.

Canada. *Personal Information Protection and Electronic Documents Act*. (2000, c.5).

Canada. *Privacy Act*, (R.S. 1985, c. P-21).

Canada. Quebec. *An Act respecting the protection of personal information in the private sector*. (c. P-39.1). Updated to 01/11/02.

Canadian Standards Association (CSA). 1996. *Model Code for the Protection of Personal Information*. CAN/CSA-Q830-96.

Carey, P. *Data protection in the UK*. London: Blackstone Press, 2000.

Carlin, F.M. The Data Protection Directive: the introduction of common privacy standards. *European Law Review*. 1996, 21(1), p.65-70.

Carter, H. Used in Europe since the last century. *The Guardian*, 04/07/02, p.6.

Cate, F.M. *Privacy in the information age*. Washington DC: Brookings Institution, 1997.

*CCN Systems Ltd v The Data Protection Registrar*, 1991; *CCN Credit Systems Ltd v The Data Protection Registrar*, 1991.

Chalton, S. et al. (eds). *Encyclopedia of data protection*. London: Sweet and Maxwell, 1988.

Clarke, R. Information technology and dataveillance. *Communications of the ACM.* 1988, 31 (5), 498-512.

Conservative party. *1979 general election manifesto.* (URL: http://www.psr.keele.ac.uk/area/uk/man/con79.htm) [Accessed 16/01/03].

Consumers International. *Privacy@net: an international comparative study of privacy on the internet.* London: Consumers International, 2001. (URL: http://www.consumersinternational.org/) [Accessed 30/11/02].

Cornford, T. The Freedom of Information Act 2000: genuine or sham? *Web Journal of Current Legal Issues* [online], 2001 (3). (URL: http://webjcli.ncl.ac.uk/2001/issue3/cornford3.html) [Accessed 30/11/02].

Council of Europe. *Convention for the protection of Human Rights and Fundamental Freedoms.* Article 8. ETS no. 005. Rome, 1950.

Council of Europe. *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector.* Strasbourg. Adopted 26/09/73.

Council of Europe. *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector.* Strasbourg . Adopted 20/09/74.

Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, ETS no. 108. Strasbourg, 1981.

Council of Europe. *Recommendation No.R (87) 15 regulating the use of personal data in the police sector.* Strasbourg. Adopted 17/09/87.

Crook, A. Data protection in the United Kingdom, part 2. *Journal of information Science.* 1983, 7 (2), 55.

Cross, M. A need to know. *The Guardian*, 14/11/02. (URL: http://www.guardian.co.uk/online/story/0,3605,839264,00.html) [Accessed 30/11/02].

Denscombe, M. *The good research guide.* Buckingham: Open University Press, 1998.

Dix, A. The German railway card: A model contractual solution of the 'adequate level of protection' issue? *18th Privacy and Data Protection Conference*, Ottawa, Canada. 18-20 September 1996. (URL: http://www.datenschutz-berlin.de/sonstige/konferen/ottawa/alex3.htm) [Accessed 16/01/03].

Dworkin, G. Privacy and the law. *In*: J.B. Young, (ed.) *Privacy*, 1978, pp.113-136.

Eaglesham, J. Industry accused of blocking data act talks. *FT.com*, 14/05/02. (URL: http://news.ft.com) [Accessed 16/01/03].

Eaglesham, J. Blunkett backs down on state e-mail snooping. *FT.com*, 18/06/02. (URL: http://news.ft.com/home/uk/) [Accessed 16/01/03].

Elliot, M. Privacy, confidentiality and horizontality: the case of the celebrity wedding photographs. *The Cambridge Law Journal.* 2001, 60 (2), 231-3.

EPIC and Privacy International. *Privacy and Human Rights 2002*, Privacy International and EPIC, 2002. (URL: http://www.privacyinternational.org/survey/phr2002) [Accessed 16/01/03].

EurActiv.com. EP plenary adopts e-communications Directive. *EurActiv.com*, 31/05/02. URL: http://www.euractiv.com [Accessed 16/01/03].

European Communities. *Treaty on European Union.* Maastricht, 1992.

European Communities. *Treaty of Amsterdam.* Amsterdam, 1997.

European Communities. Commission. *Recommendation on Implementation of Convention 108 on the Automated Processing of Personal Data.* Official Journal of the European Communities. No. L246/31. (1981).

European Communities. Commission. *Commission communication on the protection of individuals in relation to the processing of personal data in the Community.* Official Journal of the European Communities. No. C277/003. (05/11/90). COM 1990 (0314).

European Communities. Commission. *Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.* Official Journal of the European Communities. No. L281/31 (23/11/95).

European Communities. Commission. *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.* Official Journal of the European Communities. No. L024/01. (30/01/98).

European Communities. Commission. *Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related Frequently Asked Questions issued by the US Department of Commerce.* Official Journal of the European Communities. No. L215/7. (25/08/2000).

European Communities. Commission. *Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.* Official Journal of the European Communities. No. L 145/43. (31/05/2001).

European Communities. Commission. *Commission Decision 2002/2/EC of 20.12.2001 pursuant to Directive 95/46/EC of the European Parliament and of the*

*Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act*. Official Journal of the European Communities. No. L2/13. (04/01/2002).

European Communities. Commission. *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour privacy principles and related Frequently Asked Questions issued by the US Department of Commerce*. Brussels, 13/02/02. SEC (2002) 196.

European Communities. Commission. *Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community.* Official Journal of the European Communities. No. L 80/29. (23/02/2002).

European Communities. Commission. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*. Official Journal of the European Communities. No. L201/37. (31/07/02).

European Communities. Commission. DG Internal Market. *Data Protection: Background Information.* Brussels, 1998. For full text, see URL: http://europa.eu.int/comm/internal_market/en/dataprot/backinfo/info.htm [Accessed 16/01/03].

European Communities. Commission. DG Internal Market. *Opinion 8/2001 on the processing of personal data in the employment context*. Brussels. Adopted 13/09/01. (5062/01/EN/Final). WP 48.

European Communities. Commission. DG Internal Market. *Data protection: Commission recognises adequacy of Canadian regime*. Brussels. 14/01/02. (URL: http://europa.eu.int/comm/internal_market/en/dataprot/news/02_46.htm) (Accessed 16/01/03).

European Communities. Commission. DG Internal Market. *Data protection: standard contractual clauses to facilitate personal data transfers to third countries for processing*. Brussels, 22/01/02. (URL: http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/02-102.htm) [Accessed 16/01/03].

European Communities. Commission. DG XV. *First orientations on the transfers of personal data to third countries – possible ways forward in assessing adequacy.* Brussels. Adopted 26/06/97. (D/5020/97/EN/Final). WP 4.

European Communities. Commission Press Room. *Data protection at work: Commission proposes new EU framework to European social partners*. Brussels, 31/10/02. (IP/02/1593).

Davies, S. New techniques and technologies of surveillance in the workplace. *Online Rights and Privacy at Work Conference* [online], London, 28/06/99. (URL: http://www.msf-itpa.org.uk/juneconf3.shtml). [Accessed 11/12/02].

Federal Republic of Germany. Land Hessen. *Data Protection Act of 7 October 1970.*

Federal Republic of Germany. *Decision of the Federal German Constitutional Court*, Volume 65 (1983), 1ff.

Federal Republic of Germany. *Federal Data Protection Act.* 20 December 1990. Federal law Gazette I 1990, p. 2954 with amendments.

Fink, A. *How to design surveys*. Thousand Oaks, CA: Sage, 1995.

Fink, A. *Conducting research literature reviews*. Thousand Oaks, CA: Sage, 1998.

Fink, A. and J. Kosecoff. *How to conduct surveys: a step-by-step guide*. 2nd edition. Thousand Oaks, Calif: Sage, 1998.

Flaherty, D. *Protecting privacy in surveillance societies*. Chapel Hill: University of North Carolina Press, 1989.

Gardiner, J. Data traffic row intensifies. *Silicon.com*, 20/05/02. (URL: http://www.silicon.com/a53467) [Accessed 16/01/03].

Gearty, C. Incorporation of the European Convention on Human Rights; some guesses about the future. *In*: Butler, F. (ed.) *Human rights for the new millennium*. Kluwer Law International, 2000, pp.33-47.

Gellman, Robert. *Privacy, consumers and costs: how the lack of privacy costs consumers and why business studies of privacy costs are biased and incomplete.* Washington DC: EPIC, March 2002.

Gorman G.E. and P. Clayton. *Qualitative research for the information professional*. London: Library Association Publishing, 1997.

Great Britain. *Access to Medical Reports Act 1988*. London: HMSO.

Great Britain. *Anti-Terrorism, Crime and Security Act 2001*. London: TSO.

Great Britain. *Data Protection Act 1984*. London: HMSO.

Great Britain. *Data Protection Act 1998*. London: HMSO.

Great Britain. *Freedom of Information Act 2000*. London: TSO.

Great Britain. *Freedom of Information (Scotland) Act 2002*. London: TSO.

Great Britain. *Human Rights Act 1998*. London: HMSO.

Great Britain. *Local Government (Access to Information) Act 1985*. London: HMSO.

Great Britain. *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.* Statutory Instrument 2000 No. 2699. (URL: http://www.hmso.gov.uk/si/si2000/20002699.htm) [Accessed 16/01/03].

Great Britain. *Representation of the People (England and Wales) (Amendment) Regulations 2002.* Statutory Instrument 2002, No. 1871. TSO, 2002. (URL: http://www.hmso.gov.uk/si/si2002/20021871.htm) [Accessed 16/01/03].

Great Britain. Cabinet Office. *Open Government.* HMSO, 1979. (Cmnd 7520).

Great Britain. Cabinet Office. *Open Government.* London: HMSO, 1993. (Cmnd 2290).

Great Britain. Cabinet Office. *Your right to know: the government's proposals for a Freedom of Information Act.* London: HMSO, 1997. (Cmnd 3818).

Great Britain. Cabinet Office. Office of the e-Envoy. *Trust charter for electronic service delivery.* London: Office of the e-Envoy, 2001.

Great Britain. Cabinet Office. Performance and Innovation Unit. *Privacy and data-sharing: the way forward for public services.* London: PIU, 2002.

Great Britain. Department of Health. *The Caldicott Committee: Report on the review of patient-identifiable information.* London: HMSO, 1997. (URL: http://www.doh.gov.uk/confiden/crep.htm) [Accessed 16/01/03].

Great Britain. Department of Trade and Industry. *Lawful Business Practice Regulations: summary of consultation responses,* October 2000. (URL: http://www.dti.gov.uk/cii/regulatory/telecomms/telecommsregulations/lawful_business_practice_summary.shtml) [Accessed 16/01/03].

Great Britain. District Audit. *The Human Rights Act: a bulletin for public bodies.* 2002. (URL: http://www.district-audit.gov.uk/PDF/district-audit-humanrights-02.pdf) [Accessed 16/01/03].

Great Britain. Home Affairs Committee. *First report: annual report of the Data Protection Registrar*, Session 1990-1991, HC115. London: HMSO, 1990.

Great Britain. Home Office. *Report of the Committee on Privacy.* Chairman Kenneth Younger. London: HMSO, 1972. (Cmnd 5012).

Great Britain. Home Office. *Computers and Privacy.* London: HMSO, 1975. (Cmnd 6353)

Great Britain. Home Office. *Computers: Safeguards for Privacy.* HMSO, 1975. (Cmnd 6354).

Great Britain. Home Office. *Report of the Committee on Data Protection.* Chairman Sir Norman Lindop. London: HMSO, 1978. (Cmnd 7341).

Great Britain. Home Office. *Data protection: the Government's proposals for legislation.* London: HMSO, 1982. (Cmnd 8539).

Great Britain. Home Office. *Report of the Committee on Privacy and related matters*. Chairman David Calcutt. London: HMSO, 1990 (Cm 1102).

Great Britain. Home Office. *The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000, No. 191.* London: TSO.

Great Britain. Home Office. *Entitlement cards and identity fraud: a consultation paper*. London: TSO, 2002. (CM 5557). (URL: http://www.homeoffice.gov.uk/cpd/entitlement_cards.pdf) [Accessed 16/01/03].

Great Britain. Home Office: Human Rights Unit. *Human Rights Act 1998: Core guidance for public authorities: a new era of rights and responsibilities*, 2000. (URL: http://www.lcd.gov.uk/hract/coregd.htm) [Accessed 16/01/03].

Great Britain. Home Office: Human Rights Unit. *Human Rights Act 1998: Guidance for Departments.* 2nd edition, 2000. (URL: http://www.lcd.gov.uk/hract/guidance.htm) [Accessed 16/01/03].

Great Britain. House of Commons. *The Parliamentary Ombudsman Annual Report 1999-2000.* London: HMSO, 2000. (HC 593).

Great Britain. House of Commons. Select Committee on the Parliamentary Commissioner for Administration. *Second special report on open government.* London: HMSO, 1996. (HC 1995-1996 556).

Great Britain. House of Lords. *Data Protection Bill.* London: HMSO, 51. Session 1982-1983.

Great Britain. Lord Chancellor's Department. *Data Protection Act 1998: post-implementation appraisal. Summary of responses,* London: TSO, 2001. (URL: http://www.lcd.gov.uk/ccpd/dparesp.htm) [Accessed 16/01/03].

Great Britain. Lord Chancellor's Department. *Annual report on proposals for bringing fully into force those provisions of the Freedom of Information Act 2000 which are not yet fully in force.* London: TSO, 2001. (HC 367). (URL: http://www.lcd.gov.uk/foi/imprep/annrep01.htm) [Accessed 16/01/03].

Great Britain. Lord Chancellor's Department. *Data Protection Directive – European Commission's Report on Implementation. United Kingdom response to Commission questionnaire.* London: TSO, 2002.
(URL: http://www.lcd.gov.uk/ccpd/saguide.htm) [Accessed 16/01/03].

Great Britain. Lord Chancellor's Department. *Study Guide – Human Rights Act.* 2nd edition, 2002. (URL: http://www.lcd.gov.uk/hract/studyguide/index.htm) [Accessed 16/01/03].

Great Britain. Lord Chancellor's Department. *Annual report on bringing fully into force those provisions of the Freedom of Information Act 2000 which are not yet fully in force.* London: TSO, 2002. (HC6).

Great Britain. Lord Chancellor's Department. *Data Protection Directive (95/46/EC). Proposals for amendment made by Austria, Finland, Sweden and the United Kingdom. Explanatory note.* London: TSO, 2002.
URL: http://www.lcd.gov.uk/ccpd/dpdamend.htm#top [Accessed 16/01/03].

Great Britain. Office of the Data Protection Registrar. *Eleventh annual report,* London: HMSO, 1995.

Great Britain. Office of the Data Protection Commissioner. *First annual report.* London: TSO, 2000.

Great Britain. Office of the Data Protection Commissioner. *CCTV Code of Practice.* Wilmslow: Office of the Data Protection Commissioner, 2000.

Great Britain. Office of the Data Protection Commissioner. *Draft Code of Practice: The use of personal data in employer/employee relationships.* Wilmslow: Office of the Data Protection Commissioner, 2000.

Great Britain. Office of the Information Commissioner. *Data Protection Act 1998: Legal guidance.* Wilmslow: Office of the Information Commissioner, 2001.

Great Britain. Office of the Information Commissioner. *Annual Report and Accounts for the year ending 31 March 2002.* London: TSO, 2002.

Great Britain. Office of the Information Commissioner. *Freedom of Information Act 2000: An overview*. Wilmslow: Office of the Information Commissioner, 2002.

Great Britain. Office of the Information Commissioner. News release. Monitoring must be justified. *Office of the Information Commissioner*, 10/07/02.

Great Britain. Office of the Information Commissioner. *Employment Practices Data Protection Code. Part 3: Monitoring at work (Draft)*. Wilmslow: Office of the Information Commissioner, 2002.

Grossman, W. A new blow to our privacy. *The Guardian.* 06/06/02. (URL: http://www.guardian.co.uk/Print/0,3858,4427430,00.html) [Accessed 16/01/03].

The Guardian. This morning UK law sees the biggest change in more than 300 years. *The Guardian*, 02/10/00, p.1.

*Halford v United Kingdom* (1997) 24 EHRR 523.

Hall, S. and C. Dyer. Legal landmark as Naomi Campbell wins privacy case. *The Guardian,* 28/03/02. (URL: http://media.guardian.co.uk/news/story/0,7541,675295,00.html) [Accessed 16/01/03].

Hargrave, S. There's a lot of it about. *The Guardian*, 07/10/02. (URL: http://media.guardian.co.uk/Print/0,3858,4516266,00.html) [Accessed 16/01/03].

Harper, L. Model behaviour. *Privacy and Data Protection*, 2002, 3 (2), 8-9.

Harris Interactive and A. F. Westin. First major post-9/11 finds consumers demanding customers do more to protect privacy. *Harris Interactive* [online], 20/02/02. (URL: http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429) [Accessed 30/11/02].

Hart, C. *Doing a literature review.* London: Sage, 1998.

Hencke, D. and R. Evans. Blair wins battle to put open government on ice. *The Guardian*, 30/10/01. (URL: http://www.guardian.co.uk/Archive/Article/0,4273,4287729,00.html) [Accessed 16/01/03].

Hurley, N. Employers' duty of disclosure following a data subject access request. *Privacy and Data Protection.* 2002, 2 (5), 6-8.

Information Technology and People. Privacy, freedom and the Data Protection Act. *Information Technology and People.* 1983, 3 (6), 151-163.

Inman, P. Email? You've got the elbow. Jobs and Money. *The Guardian.* 25/11/00, pp.2-3.

Irvine, Lord. House of Lords, Report Stage. *Hansard HL*, London: HMSO, 585 (column 421) 29 January 1998.

Jay, R. UK Data Protection Act 1998 - the Human Rights context. *International Review of Law Computers and Technology*, 2000, 14 (3), 385-395.

Jay, R. and A. Hamilton. *Data Protection: law and practice.* London: Sweet and Maxwell, 1999.

Jonquieres, G. de. EU "no" to data privacy delay. *FT.com*, 06/05/01. (URL: http://www.ft.com) [Accessed 16/01/03].

Kearns, P. Privacy and the Human Rights Act 1998. *New Law Journal*, 16/03/01, 377-8.

Kenny, S. and J. Borking. The Value of Privacy Engineering. *The Journal of Information, Law and Technology* [online], 2002, 1. (URL: http://elj.warwick.ac.uk/jilt/02-1/kenny.html) [Accessed 17/01/03].

Kosten, F. and C. Pounder. The EC Data Protection Directive 1995: An analysis. *Web Journal of Current Legal Issues* [online], 1996, 2. (URL: http://webjcli.ncl.ac.uk/1996/issue2/kosten2.html) [Accessed 17/01/03].

Lewis, P. Silent witness: the rise of CCTV and the fall of privacy. *Independent.co.uk*, 10/09/02. (URL: http://www.independent.co.uk/story.jsp?story=331928) [Accessed 17/01/03].

Linowes, D.F. and C.J. Bennett. Privacy: its role in federal government information policy. *Library Trends*, 1986, 35 (1), 19-42.

Lloyd, I. Introduction to Data Protection Directive: special feature. *The Journal of Information, Law and Technology* [online], 1996, 1. (URL: http://elj.warwick.ac.uk/jilt/dp/introd.htm) [Accessed 17/01/03].

Lloyd, I. *A guide to the Data Protection Act 1998*. London; Edinburgh: Butterworths, 1998.

Long, W.J. and M.P. Quek. Personal data privacy protection in an age of globalisation: the US-EU safe harbor compromise. *Journal of European Public Policy*, 2002, 9(3), 325-344.

Malcolm, W. and D. Barker. Privacy and surveillance: trouble ahead for communications providers. *New Law Journal*, 2002 (7017), 80-2.

Meller, P. EU expected to reject longer data retention. *ITworld.com*, 12/11/01. (URL: http://www.itworld.com/Man/2681/IDG011112EUdataprotection/) [Accessed 16/01/03].

Mellors, C. and D. Pollitt. Legislating for privacy: data protection in Western Europe. *Parliamentary Affairs*, 1984, 37 (2), pp.199-215.

Michael, J. *Privacy and human rights: an international and comparative study with special reference to developments in information technology.* Brookfield, VT: Dartmouth, 1994.

Middleton, R. and D. Callaghan. European facelift for E-communications data privacy. *Privacy and Data Protection*, 2002, 2 (7), 3-6.

Miller, A. *The assault on privacy.* Ann Arbor: University of Michigan Press, 1971.

Mohammed, E. An examination of surveillance technology and their implications for privacy and related issues - the philosophical legal perspective. *The Journal of Information, Law and Technology* [online], 1999 (2). (URL: http://elj.warwick.ac.uk/jilt/99-2/mohammed.html) [Accessed 17/01/03].

Moore, N. *How to do research.* 3rd edition. London: Library Association Publishing, 2000.

Napier, B. Data protection begins to bite. *New Law Journal*, 1991, 141, 497-8.

New Scientist. 'The public is sick to death'. *New Scientist*, 13/10/77, p.92.

Nua surveys. More Americans online, but trust still an issue. *Nua.com*, 17/10/02. (URL: http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905358466&rel=true) [Accessed 17/01/03].

Nugter, A.C.M. *Transborder flow of personal data in the EC.* Deventer/Boston: Kluwer, 1990.

Oppenheim, C. and J.E. Davies. *Guide to the practical implementation of the Data Protection Act 1998.* London: BSI, 1998.

Organisation for Economic Cooperation and Development. *Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data.* Paris. Adopted 23/09/80.

Palmer, S. Human rights: implications for labour law. *Cambridge Law Journal,* 2000, 59 (1), 168-200.

Pearce, G. and N. Platten. Achieving personal Data Protection in the European Union. *Journal of Common Market Studies*, 1998, 36 (4), 529-547.

Pleming, N. Assessing the Act: a firm foundation or a false start? *European Human Rights Law Review*, 2000, 6, 560-579.

Pounder, C. The data protection problem. *Management Today*, 1985, pp. 39, 43, and 46.

Privacy and Data Protection. Naomi Campbell wins damages in landmark privacy ruling. *Privacy and Data Protection*, 2002, 2 (5), 1, 13.

Privacy and Data Protection. New regulations on electoral role data spell doom for marketers. *Privacy and Data Protection*, 2002, 2 (6), 1, 13.

Privacy and Data Protection. Robertson commences new action against local authority. *Privacy and Data Protection*, 2002, 3 (1), 16.

Privacy Exchange. *Transborder personal data flows: administrative practice.* URL: http://www.privacyexchange.org/tbdi/pdataflow.html [Accessed 16/01/03].

Privacy Laws and Business (International). EU DP Directive review. *Privacy Laws and Business (International)*, 2002, 65, 6-8;

Privacy Laws and Business (International). EU directive on workers' data. *Privacy Laws and Business (International)*, 2002, 65, 13-14.

Privacy Laws and Business (UK). How Barclays human resources is implementing the new Data Protection Act. *Privacy Laws and Business (UK)*, 2001, 4, 10-12.

Privacy Laws and Business (UK). How the London Clinic piloted the DPA Audit Manual. *Privacy Laws and Business (UK)*, 2001, 4, 19-21.

Privacy Laws and Business (UK). Marks and Spencer – raising staff awareness. *Privacy Laws and Business (UK)*, 2002, 7, 6-8.

Prosser, W. Privacy. *California Law Review*, 1960, 48, 383-423.

Raab, C.D. Police cooperation: the prospects for privacy. *In*: M. Anderson and M. de Boer (eds). *Policing Across National Boundaries*. London: Pinter, 1994, pp. 121-136.

Raab, C.D. Implementing data protection in Britain, *International Review of Administrative Sciences*, 1996, 62 (4), p. 498.

Raab, C.D. Co-producing data protection. *International Review of Law Computers and Technology*, 1997, 11 (1), 11-24.

Raab, C.D. From balancing to steering: new directions for data protection. *In*: Bennett, C.J., and R. Grant (eds). *Visions of Privacy*. Toronto: University of Toronto Press, 1999, pp.68-93.

Raab, C.D. European-wide sectoral codes soon to be a reality. *Privacy Laws and Business (International)*, 1999, 50, 10-12, 20.

Raab, C.D. Electronic service delivery in the UK: pro-action and privacy protection. *In*: Prins, J.E.J. (ed). *Designing e-Government: on the crossroads of technological innovation and institutional change*. Boston and The Hague: Kluwer Law International, 2001.

Raab, C.D. and C.J. Bennett. Protecting privacy across borders: European policies and prospects. *Public Administration*, 1994, 72, 95-112.

Raab, C.D. and C.J. Bennett. Taking the measure of privacy: can data protection be evaluated? *International Review of Administrative Sciences*, 1996, 62 (4), pp. 535-556.

Raab, C.D. *et al. Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: test of the method on several categories of transfer.* Final report. Luxembourg: Office for Official Publications of the European Communities. September 1998. DG XV.

Rawstorne, T. Bosses can sack staff over emails. *The Daily Mail*, 2000 pp.1-2.

Reidenberg, J.R. The globalisation of privacy solutions: the movement towards obligatory standards for fair information practices. *In*: C.J. Bennett and R. Grant (eds). *Visions of Privacy*. Toronto: University of Toronto, 1999, pp. 217-228.

Reidenberg, J.R. Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review*, 2000, 52 (5), 1315-1371.

Riley, T. UK minister discusses data protection proposals: interview with Rt Hon. Timothy Raison, Minister of State for the Home Office. *Transnational Data Report*, 1982, 5 (8), 380-382.

Rosenbaum, A. and R. MacMillan, EC data protection amendment could help heal rift with US. *Newsbytes*, 31/01/02. URL: http://newsbytes.com/news/02/174125.html [Accessed 16/01/03].

*Rotaru v Romania* (2000). Application No. 28341/95, 4 May 2000.

Rule, J.B. *Private lives and public surveillance*. London: Allen Lane, 1973.

Rule, J. et al. *The politics of privacy.* New York: Mentor, 1980.

Seipel, P. Comments on the EC Data Protection, the view from Sweden. *The Journal of Information, Law and Technology* [online], 1996, 1. URL: http://elj.warwick.ac.uk/jilt/DP/1sweden/default.htm [Accessed 16/01/03].

Shaffer, G. Globalization and social protection: the impact of EU and international rules in the ratcheting up of US privacy standards. *Yale Journal of International Law,* 2000, 25 (1), 1-88.

Sieghart, P. *Privacy and computers*, London: Latimer, 1976.

Simitis,S. Reconsidering the premise of labour law: prolegomena to an EU regulation on the protection of employees personal data. *European Law Journal*, 1999, 5 (1), 45-62.

Singh, R. Privacy and the media after the Human Rights Act. *European Human Rights Law Review*, 1998, 6, pp. 712-729.

Singh, R. and J. Strachan. The right to privacy in English law. *European Human Rights Law Review*, 2002, 2, pp. 129-161.

Singleton, S. *Data Protection: the new law.* Bristol: Jordans, 1998

*Sunday Times v United Kingdom* (1979) 2 EHRR 245;

Sweden. *Personal Data Act 1998.* Swedish Code of Statutes, SFS 1998: 204.

Sweden. Data Inspection Board. *Annual Report 1999.* Stockholm: Data Inspection Board, 1999.

Tendler, S. Yard's new computer to hold 1.3 million criminal files. *The Times*, 14/02/77, p.2;

Tendler, S. Special branch to put suspects' names on computer file. *The Times*, 09/09/77, p.1.

Thomas, S. Privacy: media. *Privacy and Data Protection*, 2001, 1 (3), 8-9.

Thompson, B. Every click you make. Online. *The Guardian*, 02/11/00, pp. 2-3.

The Times. Leader: Liberty takes a back seat. *The Times*, 12/02/83, p.9.

UNICE. *UNICE position on Commission's first stage consultation on the protection of worker's personal data*. Brussels: UNICE, 30/10/01.

UNICE. *Commission's second-stage consulation on the protection of workers' personal data. UNICE's reply*. Brussels: UNICE, 06/01/03.

University of Hull. Information Law and Technology Unit. *JISC Data Protection Code of Practice for the HE and FE Sectors*. Version 2.0, 2000. Refer: URL: http://www.jisc.ac.uk/pub00/dp_code.html [Accessed 16/01/03].

United Nations. *Universal Declaration of Human Rights 1948*. United Nations Publications: New York.

United States. *Federal Trade Commission Act*. 15 USC 41-51, 1914.

United States. *Freedom of Information Act*, 5 USC 552, 1966.

United States. *Privacy Act*, 5 USC 552a, 1974.

United States. Federal Trade Commission. *Public workshop: the mobile wireless web, data services and beyond: emerging technologies and consumer issues*. Washington DC: FTC, February 2002;

United States. Privacy Protection Study Commission. *Personal Privacy in the Information Society*, 1977. Washington: US Government Printing Office, 20402.

United States Supreme Court. *NAACP v. Alabama*, 357 US 449 (1958).

United States Supreme Court. *Griswold v. Connecticut*, 381 US 479 (1965).

United States Supreme Court. *Katz v. US*, 386 US 954 (1967).

United States Supreme Court. *Roe v. Wade*, 410 US 113 (1973).

United States Supreme Court. *Federal Aviation Administration Robertson v. Robertson*, 422 US 255 (1975).

University of Strathclyde. ENLIST project. *Data Protection and Privacy – Commentary*. University of Strathclyde, 2000. (URL: http://itlaw.law.strath.ac.uk/ENLIST/subjects/dpp/commentary/) [Accessed 16/01/03].

Van der Donk, W.B.H.J. and H.P.M. van Duivenboden. Privacy as a policy: policy implementation perspective on data protection at shopfloor level in the Netherlands. *International Review of Administrative Sciences*, 1996, 62 (4), 513-534.

Veitch, A. Data protection under fire from all sides. *The Guardian*, 16/09/81, p.2.

Wadham, J., J. Griffiths and B. Rigby. *Freedom of Information Act 2000*. London: Blackstone Press, 2001.

Wadham, J. and H. Mountfield. *Human Rights Act 1998*, London: Blackstone, 1998.

Warren, A. Right to privacy? The protection of employee personal data in the UK. *Proceedings: 10th international BOBCATSSS symposium on library and information science*, Portoroz, Slovenia. 28-30 January 2002, pp. 71-79.

Warren, S.D. and Brandeis, L.D. The right to privacy. *Harvard Law Review*, 4, 1890, 193-220.

Weardon, G. US tech protests EU privacy laws. *ZDNet*, 30/09/02. (URL: http://zdnet.com.com/2100-1106-960134.html) [Accessed 16/01/03].

West Midlands Local Authorities Data Protection Forum. *Data Protection Code of Practice*. Sandwell: Sandwell MBC, 2001.

Westin, A.F. *Privacy and freedom*. New York: Atheneum, 1967.

Widdison, R. Data protection law: the key changes. *Web Journal of Current Legal Issues* [online], 1998, 4. (URL: http://webjcli.ncl.ac.uk/1998/issue4/widdis4.html) [Accessed 16/01/03].

Wiebe, A. Harmonisation of data protection law in Europe. Report on the working conference on EC Data Protection Directive. *The Journal of Information, Law and Technology* [online], 1996, 3. (URL: http://elj.warwick.ac.uk/jilt/confs/3dp/default.htm) [Accessed 16/01/03].

Williams, K. Re-regulating free speech: privilege, public interest and privacy. *Web Journal of Current Legal Issues* [online], 1999, 1. (URL: http://webjcli.ncl.ac.uk/1999/issue1/williams1.html) [Accessed 16/01/03].

Wood, S. and J. Dearnley. Open government? Freedom of information legislation and information provision in the UK. *Proceedings of 8th International BOBCATSSS Symposium on Library and Information Science, Krakow, Poland.* 24-26 January 2000, pp. 307-317.

Wolverton, T. Privacy groups target Amazon again. *News.com*, 08/10/02. (URL: http://news.com.com/2102-1017-961136.html) [Accessed 30/11/02].

Yin, R. *Applications of case study research.* Newbury Park, CA: Sage, 1993.

Youngman, M.B. Designing and using questionnaires. *In* Bennett, N., R. Glatter, and R. Levacic, (eds). *Improving educational management*. London: Paul Chapman, 1994.

# Appendix A

## Interview: Sir Norman Lindop – 6 September 2001

# Interview: Sir Norman Lindop - 6 September 2001

Appropriately, the first expert interview was with Sir Norman Lindop, chairman of the Data Protection Committee, whose report in 1978 commenced serious moves in the UK towards legislating for data protection. The interview thus provided a fascinating insight into the history behind the current UK data protection regime. The Lindop Report, as discussed in Chapter 4 (section 4.5.3), was a comprehensive study into the practices of organisations in both the public and private sectors when using personal data. Lindop was approached to chair the Committee in June 1976, whilst director of Hatfield Polytechnic, following the sudden death of the original candidate, Sir Kenneth Younger. After receiving the request "out of the blue" from the then Home Secretary, Roy Jenkins, Lindop acquired copies of the Younger Report[1] and the 1975 White Paper *Computers and Privacy*[2] from the Polytechnic library, and took them home to read over the weekend. On the Monday, he rang the Home Secretary's office, saying: "I don't know anything about this". To which, Lindop related, the reply was:

> ""That's neither a disqualification, nor a reason for not doing it," and basically, get on with it!"

At interview, Lindop stated he was unsure why he was approached in the first place, although he commented: "the fact that Hatfield was very prominent in computer education at that time may have had something to do with it".

The Committee of twelve comprised six specialists in areas relevant to privacy and information technology, and six so-called "lay people", including the chairman himself. This arrangement was deemed by the interviewee to have been successful. The two key experts on the Committee were Paul Sieghart and Charles Read – both now deceased. The former was a barrister, a human rights advocate, and had been involved in bringing together the members of the Committee other than the chairman. A hugely talented individual, Sieghart had "somehow got the ear of Roy Jenkins", and had been employed by the Home Office to write the White Paper *Computers and Privacy* – a "very good starting document" for the

Committee. Read, director of the Inter-Bank Research Organisation, was "first rate" and "an excellent Committee man".

The Committee was established to formulate principles on which future data protection legislation should be based. Following on from the work of the Younger Committee on Privacy, the Data Protection Committee was "welcomed by a large number of people". Initially, Lindop had hoped that the Committee's work would take a year, but it took twice that period:

> "That was partly because the gathering of information took longer than we expected. We also had to do one or two investigations on the spot."

The latter included a trip to Sweden, a home of the first national data protection law; and attendance of a Council of Europe meeting in Vienna. The Swedish visit, conducted in December 1976, demonstrated to the Committee that "the data protection regime could work". On a lighter note, Lindop observed that although the Stockholm health system had data subject access:

> "...the only thing people ever tried to change was their address! There was never any upset over the medical diagnosis or anything like that."

This impressed on the interviewee, as issues that appear to be matters of principle can turn out to be rather inconsequential.

However, at the same time, the work of the Committee was "resisted" in certain quarters:

> "It was not resistance in the physical form, or political sense, although I suppose it was political. It was more as to be cautious in what we recommended because of the implications."

Organisations that were more defensive included the secret service and the police. The former did not reply to the Committee's enquiries, whilst the police "came and put up a witness who refused to answer any questions!" As a result, the

Committee had to rely on press revelations in *The Times* by investigative journalist Stewart Tendler concerning the Police National Computer[3].

In a general discussion concerning data protection issues that had emerged since publication of the Lindop Report in 1978, the interviewee made two observations. Firstly, that the private sector – due to the growth of multi-national corporations - has emerged as a much greater threat than was anticipated during the mid-1970's. With hindsight, the interviewee believed the Committee were "naïve" about that:

> "We were very pre-occupied with the threat which we saw being presented by government departments, and we didn't see the private sector as being a threat. "

Secondly, the issue of who has 'control' over electronic information was raised. In this respect, Lindop admitted to feeling "a bit despondent", and had difficulty in perceiving how "any degree of data protection can be offered to anyone at this particular time":

> "It used to be technically feasible at least to say that you could destroy information if it was printable, but you can't control electronic information once you have released it."

This interview provided excellent context and insight to the issues explored in later expert interviews. The perspective of one of the key forces behind the first UK Data Protection Act was particularly illuminating, enabling desk research to be triangulated with human observation. As stated in Chapter 2, the author attempted to acquire papers relating to the work of the Data Protection Committee for Loughborough University's Department of Information Science, only to be prevented by the law relating to disposal and preservation of public records (refer to Home Office letter, Appendix B).

## References


[1] Great Britain. Committee on Privacy. *Report of the Committee on Privacy.* Chairman Kenneth Younger. HMSO, 1972. (Cmnd 5012).

[2] Great Britain. Home Office. *Computers and Privacy.* HMSO, 1975. (Cmnd 6353).

[3] Refer:

- Tendler, S. Yard's new computer to hold 1.3 million criminal files. *The Times*, 14/02/77, p.2;
- Tendler, S. Special branch to put suspects' names on computer file. *The Times*, 09/09/77, p.1.

# Appendix B

Copy of Home Office letter dated 15 November 2001

re Lindop papers

# Home Office

**Record Management Services**
Corporate Support Services Unit

50 Queen Anne's Gate, London SW1H 9AT
Switchboard 020 7273 4000 Fax 020 7273 3592 Direct Line 020 7273 2150
E-mail Tim.Sargent@homeoffice.gsi.gov.uk www.homeoffice.gov.uk

Our Ref
Your Ref
Date 15 November 2001

Mr Adam Warren
Department of Information Science
Loughborough University
Leicestershire
LE11 3TU

Dear Mr Warren

**HOME OFFICE COMMITTEE ON DATA PROTECTION**

Thank you for your letter of 27 October.

The official records relating to the Home Office Committee on Data Protection are held at the Public Record Office in the Home Office class HO261. Some papers are open to public inspection but others remain closed for 30 years and therefore those from the final stages of the committee in 1978 are not due to be released until January 2009.

I have consulted the Public Record Office about your Department's intention to acquire Sir Norman Lindop's papers for the purposes of placing them in an open archive which would be accessible to all students. We are advised that this would be unwise as it is not good practice to have duplicate sets of papers and the Public Record Office is the correct place of deposit for such records. If Sir Norman wishes to dispose of his papers, the best course of action would be to offer them to the Home Office and we would ensure that any which were not already held at the Public Record Office were transferred for permanent preservation.

Yours sincerely

Tim Sargent
Head of Record Management Services



V11

# Appendix C

## Pilot Questionnaire

*Privacy and human rights in the workplace*

# Privacy and Human Rights in the Workplace

Respondent's identities will be kept confidential. The ID number at the top will be used only to track response rates.

Please return your completed questionnaire by **Friday 2 March 2001**.
A pre-paid envelope is enclosed.

## A. Data Protection

**A1. Does your organisation have a nominated member of staff with responsibility for data protection?**

*Please tick.* (✓)

Yes ☐
No ☐

**A2. What steps has your organisation taken to comply with the Data Protection Act 1998?**

*Please tick those that apply:* (✓)

- Internal audit ☐
- Staff training (in-house) ☐
- Staff training (external) ☐
- Policy on employee personal privacy ☐
- Policy on automated decision-making ☐
- Policy on subject access requests ☐

- Other, *please specify* ☐

**A3. What are the procedures for dealing with subject access requests?**
(These are requests made by users of your services for data concerning themselves.)

## B. Privacy policies

| | Yes (✓) | No (✓) |
|---|---|---|
| **B1. Does your organisation's website require users to disclose personal data to you?** *If no, proceed to section C.* | ☐ | ☐ |
| **B2. *If yes*, does your organisation's website have a privacy statement?** *If no, proceed to section C.* | ☐ | ☐ |
| *If yes*: | | |
| - Does that statement include: | | |
| (i) Right of access to personal data | ☐ | ☐ |
| (ii) Right to have inaccurate data corrected or deleted | ☐ | ☐ |
| (iii) Transfer of data to third (non-EU) countries | ☐ | ☐ |
| (iv) Opt-out from receiving marketing material | ☐ | ☐ |

**B3. Is the privacy statement on the main page, or does the user have to hyperlink to it?**

| | |
|---|---|
| Main page | ☐ |
| Hyperlink | ☐ |

## C. Monitoring of employees

| | Yes (✓) | No (✓) |
|---|---|---|
| **C1. Does your organisation have a formal policy concerning staff use of:** | | |
| (i) Email | ☐ | ☐ |
| (ii) Internet | ☐ | ☐ |
| **C2. Does your organisation monitor staff use of:** | | |
| (i) Email | ☐ | ☐ |
| (ii) Internet | ☐ | ☐ |
| *If no to both C2 (i) and (ii), proceed to C5.* | | |

**C3. How frequently does your organisation monitor use of email and/or the Internet?**

| | (✓) | | (✓) |
|---|---|---|---|
| Daily | ☐ | Less than | ☐ |
| Weekly | ☐ | once/month | |
| Fortnightly | ☐ | Only when good | |
| Monthly | ☐ | reason to do so | ☐ |

**C4. Is Email/Internet use monitored automatically?**

*Please tick* (✓)

| | |
|---|---|
| Yes | ☐ |
| No | ☐ |

*If yes*, please give details of software used:

.....

.....

.....

.....

**C5. Has your organisation obtained the Data Protection Commissioner's *Draft code of practice on the use of personal data in employer/employee relationships*?**

| Yes (✓) | No (✓) |
|---|---|
| ☐ | ☐ |

*If no, proceed to D1.*

*If yes:*

| | | Yes (✓) | No (✓) |
|---|---|---|---|
| (i) | Was the scope of the Code clear? | ☐ | ☐ |
| (ii) | Are the standards clear? | ☐ | ☐ |
| (iii) | In your opinion, does it impose disproportionate burdens on your organisation? | ☐ | ☐ |

*If yes* to (iii), please give reasons:

.....

.....

.....

.....

.....

## D. Other legislation

**D1. Is your organisation aware of the Department of Trade and Industry's *Lawful business practice regulations*?**
*If no, proceed directly to D2(ii).*

| Yes (✓) | No (✓) |
|---|---|
| ☐ | ☐ |

**D2. Please indicate the degree to which you agree with the following statements**

1 indicates you strongly agree 3 indicates you neither agree nor disagree

5 indicates strong disagreement

*Please circle most appropriate number.*

(i) The *Lawful Business Practice Regulations* complement the *Draft code of practice on the use of personal data in employer/employee relationships*

Don't know/No opinion

1 2 3 4 5 ☐

(ii) The Data Protection Act 1998 represents a positive measure for ensuring compliance and good practice.

Don't know/No opinion

1 2 3 4 5 ☐

(iii) The Human Rights Act 1998 will have a considerable impact on our organisation's handling of personal data.

Don't know/No opinion

1 2 3 4 5 ☐

(iv) The Human Rights Act will work effectively in tandem with the Data Protection Act 1998. Overlap is minimal and meaning is clear.

Don't know/No opinion

1 2 3 4 5 ☐

**D3. Any further comments:**

# Appendix D

## Full Questionnaire

*Privacy and human rights in the workplace*

# Privacy and Human Rights in the Workplace

Respondent's identities will be kept confidential. The ID number at the top will be used only to track response rates.

Please return your completed questionnaire by **Friday 12 October 2001.**
A pre-paid envelope is enclosed.

## Data Protection

**1 Does your organisation have a nominated member of staff with responsibility for data protection?**

| | Yes | No |
|---|---|---|
| *Please tick.* (✓) | ☐ | ☐ |

**2 What steps has your organisation taken to comply with the Data Protection Act 1998?**

| *Please tick those that apply:* | (✓) |
|---|---|
| - Internal audit | ☐ |
| - Staff training (in-house) | ☐ |
| - Staff training (external) | ☐ |
| - Policy on employee personal privacy | ☐ |
| - Policy on automated decision-making | ☐ |
| - Policy on subject access requests | ☐ |

- Other, *please specify* ☐

.....

.....

.....

.....

## Employee Records

**3 For what purposes is personal information collected from employees by your organisation?**

.....

.....

.....

.....

.....

.....

**4** **Are staff informed of these purposes?** Yes ☐ No ☐

*Please tick* (✓)

*If yes, how are staff informed?*

**5** **How is the accuracy of employees' personal data checked and maintained?**

**6** **For how long are the following employee records kept:**

| | |
|---|---|
| Application forms | |
| References received | |
| Payroll and tax | |
| Sickness | |
| Annual appraisal/assessment | |
| Accident/injury at work | |
| Promotion, transfer, training and discipline | |
| References given | |
| Summary of record of service e.g. name, position held, dates of employment | |

**7** **What are the subject access procedures for employees asking to view their records?** *Please append if necessary.*

**8 What are the security procedures in place for safeguarding employee records?**

| *Please tick those that apply:* | (✓) |
|---|---|
| - Adherence to security standards e.g. BS 7799 | ☐ |
| - Access controls to employee records | ☐ |
| - Password controls to employee records | ☐ |
| - Disciplinary procedures for unauthorised access to employee records | ☐ |
| - Encryption of emails transferring employee data | ☐ |

- Other, *please specify* ☐

.....

.....

.....

.....

.....

## Employee Monitoring

| **9 Does your organisation have a formal policy concerning staff use of:** | Yes (✓) | No (✓) |
|---|---|---|
| (i) Email | ☐ | ☐ |
| (ii) Internet | ☐ | ☐ |

| **10 Does your organisation monitor staff use of:** | | |
|---|---|---|
| (i) Email | ☐ | ☐ |
| (ii) Internet | ☐ | ☐ |

*If no to both 9 and 10, please proceed to 13.*

**11 How frequently does your organisation monitor use of email and/or the Internet?**

| | (✓) | | (✓) |
|---|---|---|---|
| Daily | ☐ | Less than once/month | ☐ |
| Weekly | ☐ | | |
| Fortnightly | ☐ | Only when good reason to do so | ☐ |
| Monthly | ☐ | | |

**12 Is Email/Internet use monitored automatically?**

| | Yes | No |
|---|---|---|
| *Please tick* (✓) | ☐ | ☐ |

*If yes*, please give details of software used:

.....

.....

.....

.....

## Legislation and official guidance

| **13 Is your organisation aware of:** | Yes (✓) | No (✓) |
|---|---|---|
| - the Information Commissioner's *Draft code of practice on the use of personal data in employer/ employee relationships* | ☐ | ☐ |
| - the Department of Trade and Industry's *Lawful business practice regulations* | ☐ | ☐ |
| - the Human Rights Act 1998 | ☐ | ☐ |

**14 Please indicate the degree to which you agree with the following statements**

1 indicates you strongly agree
3 indicates you neither agree nor disagree
5 indicates strong disagreement
*Please circle most appropriate number.*

(i) *The Lawful Business Practice Regulations* represent a positive measure for ensuring compliance and good practice.

| 1 | 2 | 3 | 4 | 5 | Don't know/No opinion ☐ |
|---|---|---|---|---|---|

(ii) The Data Protection Act 1998 represents a positive measure for ensuring compliance and good practice.

| 1 | 2 | 3 | 4 | 5 | Don't know/No opinion ☐ |
|---|---|---|---|---|---|

(*Continued overleaf*)

(iii) The Human Rights Act 1998 will have a considerable impact on our organisation's handling of personal data.

1 2 3 4 5 Don't know/No opinion ☐

(iv) Official guidance concerning the Data Protection Act 1998 has been clear and practical.

1 2 3 4 5 Don't know/No opinion ☐

(v) Official guidance concerning the Human Rights Act 1998 has been clear and practical.

1 2 3 4 5 Don't know/No opinion ☐

**15 Any further comments:**

It is intended that follow-up interviews will be conducted with some organisations later in the year. If interested, *please supply contact details in the box below:*

Thank you for your time.

You cooperation in this study is appreciated.