Chapter 4
United Kingdom

Contents

1 INTRODUCTION

Although common law and constitutional law may indirectly protect information or data privacy in the UK, data protection is provided essentially through legislation, and in particular through the Data Protection Act of 1998. The first Data Protection Act was adopted in 1984. In 1998 a new Data Protection Act was adopted, because the UK, like the rest of the European Union countries, had to bring the provisions of its legislation into line with the European Union Directive on data protection.[1]

Before discussing the Data Protection Act of 1998, brief reference will be made to the protection of privacy in common law and constitutional law.

2 PROTECTION OF PRIVACY IN COMMON LAW

Traditionally, English law does not recognise a general right to privacy under common law.[2] An English court held in 1991:

---

1 Dir 95/46/EC (see Int ch par 4). Hereafter referred to as "the Directive".

2 Rogers *Winfield & Jolowicz on torts* 464; Neill *Privacy* 17; Lloyd *Information technology law* 29; Neethling *Privaatheid* 241; Sterling *Data Protection Act* 12; Michael *Privacy and human rights* 100; Campbell *Data transmission and privacy* 107; Rumbelow 1984 *Int Bus L'yer* 153. This is also the position in Wales. In Scotland, however, the largely civil legal system has moved further towards recognising a general right to privacy by means of the *actio iniuriarum* which provides a remedy for injuries to honour (Michael *Privacy and human rights* 100. Also see Chalton et al *Encyclopedia of data protection* par 1–020).

However, there is still support for the notion that a tort of privacy infringement should be recognised in the UK. See eg David Calcutt *Review of press self-regulation* HMSO 1993 (Sir David Calcutt previously – in 1990 – chaired the Committee on Privacy which rejected the introduction of a new tort on infringement of privacy) and the Lord Chancellor's consultation paper (July 1993) both quoted in Milmo 1993 *New LJ* 1182; Goodenough 1993 *Eur Intel Prop R* 227. However, in 1995 the government announced in response to the 1993 consultation paper as well as a report by the National Heritage Select Committee recommending a privacy bill that it had no plans to introduce a statutory right of privacy (see *Privacy and media intrusion* Cmnd 2918 quoted in Jay & Hamilton *Data protection* 266–267).

> It is ... invasion of privacy which underlies the plaintiff's complaint. Yet it alone, however gross, does not entitle him to relief in English law.[3]

Ten years on, it remained the view of a Court of Appeal that

> [T]here is no tort of invasion of privacy. Instead there are torts protecting a person's interests in the privacy of his body, his home and his personal property. There is also the equitable doctrine of breach of confidence for the protection of personal information, private communications and correspondence.[4]

Common law can indirectly protect privacy in personal information by means of established remedies which provide protection against unauthorised disclosure or misuse of information.[5] Examples of such remedies are breach of confidence,[6] conspiracy,[7] copyright,[8] breach of contract,[9] negligence,[10]

3 *Kaye v Robertson* [1991] FSR 62, 70 (per Glidewell, LJ). See also *Malone v Metropolitan Police Commissioner (No2)* [1979] 2 All ER 620. In the *Malone* case Sir Robert Megarry held that English law did not recognise a right to privacy and that the tapping of a telephone conversation by the Post Office could therefore not amount to a breach of such a right. Also see fn 19.

4 *R (on the application of Wainwright) v Richmond upon Thames London Borough Council* [2001] EWCA Civ 2062, CA. See also Carey *E-Privacy* 3.

5 See in general Neethling *Privaatheid* 245 *et seq*; McQuoid-Mason *Privacy* 50 *et seq*.

6 The action for breach of confidence may be available if information "impressed with confidence" is used or disclosed without authorisation. Damages can be claimed to compensate for loss flowing from the breach. According to Rogers *Winfield & Jolowicz on torts* 467, in practice the law of confidence is by far the most important legal mechanism and the one which comes closest to considering privacy issues directly. (See *Prince Albert v Strange* (1849) ER 1171; *Duchess of Argyll v Duke of Argyll* 1967 Ch 302; *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804; Rogers *Winfield & Jolowicz on torts* 467–469; Wacks *Personal information* 50–134; Neill *Privacy* 8–10; Sterling *Data Protection Act* 12; Chalton et al *Encyclopedia of data protection* par 1–015.) Recently a Court of Appeal recognised for the first time that a legal right of privacy is capable of existing in English law independently of the law of confidential information. The case involved the celebrity wedding of Michael Douglas and Catherine Zeta-Jones. The couple obtained an interim interdict against a magazine preventing the magazine from publishing photographs of their wedding (*Douglas v Hello! Ltd* [2001] QB 967, [2001] 2 WLR 992, [2002] 1 FCR 289, [2001] 1 FLR 982, CA). In the *Douglas* case the court stated that it had taken into account the provisions of the Human Rights Act 1998 and a 8 of the European Convention on Human Rights (see par 3).

7 The action for conspiracy requires an agreement between two or more persons to injure another, otherwise than in the furtherance of their legitimate pursuits. If personal information is misused in these circumstances it would, incidentally, also be protected (Chalton et al *Encyclopedia of data protection* par 1–018).

8 The action for breach of copyright is a statutory remedy which protects the work produced by the (continued...)

trespass,[11] legal professional privilege,[12] and certain statutory remedies.[13] The Data Protection Act of 1998 does not abolish any of these remedies, but the protection provided by them to privacy in personal information is incidental and limited.[14]

8(...continued)
copyright owner, and as a consequence could also protect the privacy of information contained therein. Rogers *Winfield & Jolowicz on torts* 467 gives the example of *Williams v Settle* [1960] 1 WLR 1072. "In this case the plaintiff's father-in-law had been murdered in circumstances which attracted publicity. The defendant, who had taken the photographs at the plaintiff's wedding two years previously, sold one for publication in the national press. The copyright in the photographs was the plaintiff's and therefore the court was able to award him heavy damages for the defendant's 'scandalous conduct' which was 'in total disregard not only of the legal rights of the plaintiff regarding copyright but of his feelings and his sense of family dignity and pride'. Under current copyright law the rights in such a photograph would probably be in the photographer but, ironically, this is one instance in which the law does address the issue of privacy head on, for under s 85 of the Copyright, Designs and Patents Act of 1988, breach of which is actionable as a breach of statutory duty, a person who for private and domestic purposes commissions the making of a photograph or film has the right to prevent the issue of copies to the public."

9 The action for breach of contract is only available if a contract existed between the parties, and the defendant's disclosure of information in breach of the contract caused the plaintiff damage. Punitive or general damages is not available. Once again the relevance to privacy protection is incidental (Chalton et al *Encyclopedia of data protection* par 1-017). When the Princess of Wales was photographed without her consent exercising in a gymnasium, her lawyer chose breach of contract and breach of confidence as causes of action (see Singleton 1995 *Computer L & Prac* 140; Fenwick & Phillipson 1996 *Cambridge L J* 447 449).

10 The action for damages resulting from negligence will indirectly protect privacy in information if there was a disclosure of personal information giving rise to loss where the disclosure has resulted from breach of a duty of care and where the loss was reasonably foreseeable (Chalton et al *Encyclopedia of data protection* par 1-017).

11 Trespass is the unauthorised physical interference with a person's property, person or goods and may give rise to a cause of action and a remedy in damages. Interference with information as such will not be an actionable trespass, but trespass to a person's documents can give rise to such an action and thus indirectly protect any personal information contained therein (Chalton et al *Encyclopedia of data protection* par 1-016). Also see Neill *Privacy* 4–5.

12 Legal professional privilege applies to all information passed between attorney and client, and thus also protects personal information passed in this way. However, the purpose is to secure the proper pursuit of justice and not to protect privacy (Chalton et al *Encyclopedia of data protection* par 1-018).

13 Eg, the purpose of the Official Secrets Act of 1989 is to protect state secrets. Personal information forming part of this will also be protected. The Post Office (Data Processing Services) Act of 1967 makes it an offence to improperly disclose information about the use made of telecommunications services and can also in a limited way protect privacy in personal information. Other legislation to bear in mind is the Interception of Communications Act of 1985, the Telecommunications Act of 1984 (ss 43(1)(b) and s 45), the Wireless Telegraphy Acts of 1967 and 1969 and the Post Office Acts of 1963 and 1969. Also see the Human Rights Act of 1998 discussed in par 3. See also Chalton et al *Encyclopedia of data protection* par 1-019.

14 According to 1972 *Int Soc Sci J* 457 an "...inevitable consequence of the fortuitous character of these (continued...)

3 PROTECTION OF PRIVACY UNDER CONSTITUTIONAL LAW: HUMAN RIGHTS ACT OF 1998

3.1 Introduction

It is usually said that the UK does not have a written constitution. In one sense this is true, but such a statement obscures the fact that there is legal material in the form of legislation which has given some written definition to domestic constitutional arrangements.[15] The Human Rights Act of 1998 is one such legal instrument.[16]

The Human Rights Act was adopted to give effect to the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms[17] in UK law. The UK government was involved in the drafting of the European Convention on Human Rights; the UK was one of the first countries to sign it in 1950 and the first to ratify it in 1951.[18] However, at that time the UK chose not to incorporate the Convention into its national law, and the Convention could therefore not be adjudicated before UK courts.[19] Furthermore, the UK did not initially accept individual petition to the

14(...continued)
remedies is that they are inadequate to protect all aspects of privacy. As they were designed for a different purpose, it is hardly surprising if they prove at times to be ineffective shields." See also Justice *Privacy and the law* 8; Sieghart *Privacy and computers* 31.

15 See Baker *Human Rights Act 1998* 1.

16 Other examples of such materials are the Magna Carta of 1215, the Bill of Rights of 1689, the Act of Settlement of 1700, the Acts of Union of 1707 and 1801, the Parliament Acts of 1911 and 1949, the Crown Proceedings Act of 1947, and the European Communities Act of 1972 (see Baker *Human Rights Act 1998* 1; Greer 1999 *European LR* 3. Also see Slee 1999 *Inf & Comm Tech L* 71 fn 1, 72 fn 5 for comments on the Act).

17 Hereafter: "the (European) Convention on Human Rights".

18 Baker *Human Rights Act 1998* 1. The UK is also a party to other human rights codes, eg the Universal Declaration of Human Rights of 1948 and the United Nations Covenant on Civil and Political Rights of 1966.

19 Baker *Human Rights Act 1998* 4; Justice *Privacy and the law* 1; Bennett *Regulating privacy* 82. In *Malone v Metropolitan Police Commissioner* (No 2) [1979] 2 All ER 620 the court held that English law does not recognise a right to privacy and that the tapping of a telephone conversation by the Post Office can therefore not amount to a breach of such a right. The judge recognised that his decision was inconsistent
(continued...)

European Court of Human Rights, established by the Convention to enforce its provisions against member governments. In 1966 the UK government changed its position on the question of individual petition and since that date individuals who claim that their rights under the European Convention on Human Rights have been violated by the UK government have been able, once they have exhausted their domestic remedies, to take their case to the European Court of Human Rights in Strasbourg.[20]

Since the 1960s there has been an ongoing debate over the incorporation of the European Convention on Human Rights into UK law.[21] The introduction of the right to individual petition to the European Court of Human Rights contributed to the increasing impact of the European Convention on Human Rights in the UK from the 1970s onwards. The European Court of Human Rights has found the UK to be in breach of the Convention in a number of cases, and this has increased public awareness of the Convention. In time there was a shift in public opinion in favour of incorporation, and during the 1997 election campaign Tony Blair's Labour Party outlined its plans to incorporate the Convention, in a consultation paper entitled *Bringing Rights Home.* The Human Rights Act, the purpose of which was to give "further effect to rights and freedoms guaranteed under the European Convention on Human Rights" was adopted in 1998 and came into operation on 2 October 2000.[22]

3.2 Protection of privacy under Human Rights Act

The European Convention on Human Rights protects privacy in articles 8(1) and 8(2). These two

19(...continued)
with a 8(1) of the European Convention on Human Rights, but held that the fact that the Convention was not directly enforceable in England justified his decision.

20 The plaintiff in the *Malone* case (see fn 19) took his case to the European Court of Human Rights. The court held that the English practice of interception was insufficiently grounded in law to allow it to be justified under a 8(2) of the Convention. In response to this decision, the UK passed the Interception of Communications Act of 1985 and the Police Act of 1977 Part III. Other cases heard in Strasbourg include *Halford v United Kingdom* [1997] 24 ECHR 523 and *Gaskin v United Kingdom* [1989] 12 ECHR 36.

21 See House of Commons Library *Research paper 98/24* 17– 24.

22 See http://www.lawrights.co.uk/hra.html. For a discussion of the Human Rights Act, see Greer 1999 *European LR* 3.

articles form part of the Human Rights Act of 1998.[23] They guarantee that individuals have the right to respect for their private and family lives, their homes and correspondence. Public authorities may not interfere with the exercise of these rights, except where this 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.

From a data protection point of view, the protection of the right to privacy provided by this Act will be limited by the fact that the Act is only enforceable against public authorities. The Human Rights Act essentially strengthens the rights of individuals against the state.[24]

The Act's effectiveness is also limited by its implementation mechanism and weak remedial scheme. A person who feels aggrieved by an act or omission on the part of a public authority which is in contravention of any right in terms of the Convention may challenge the act or omission in court.[25] If the court finds that a public authority has acted unlawfully by failing to comply with the Convention, the authority will not be exposed to criminal penalties,[26] but the court may grant a remedy which is within its normal powers and which it considers to be appropriate.[27] An award of damages may be made only in certain narrowly defined circumstances.[28] Rights under the Convention are further put into effect in UK law by the obligation on the part of the courts to interpret legislation so as to be compatible with

23 HR Act of 1998 sch 1, part 1 aa 8(1) and (2).

24 At first sight it would appear that the use of personal information by private parties does not fall under this Act. However, there is also the view among some commentators that the Act will at least have indirect horizontal application against private individuals and companies (see Singh "Privacy and the media" 186, 190 and authority cited by him). Also see the *Douglas* case discussed above (*Douglas v Hello! Ltd* [2001] QB 967, [2001] 2 WLR 992, [2002] 1 FCR 289, [2001] 1 FLR 982, Ca) where the court stated that it had taken into account the provisions of the Human Rights Act 1998 and a 8 of the European Convention on Human Rights, although the action was not brought against the government, but against a newspaper company.

25 HR Act of 1998 s 7.

26 HR Act of 1998 s 6(7).

27 HR Act of 1998 s 8(1).

28 HR Act of 1998 ss 8(2) and (3).

the Convention rights.[29] If the legislation is incompatible with the Convention, a declaration of incompatibility may be made.[30] Such a declaration does not change the law, or its validity, or continuing operation, neither is it binding on the parties to the proceedings.[31] It is left to Parliament to change the law, which can be a time-consuming process.[32]

The importance of the Human Rights Act from a data protection perspective lies in the fact that the courts, as well as the Commissioner and the Tribunal appointed to enforce the Data Protection Act, will have to interpret the Act in a manner that is consistent with the application of the Convention rights.[33]

4 PROTECTION OF DATA PRIVACY THROUGH LEGISLATION: DATA PROTECTION ACT OF 1998

4.1 Introduction

The Data Protection Act (DP Act) of 1998 is the main source of data protection in the UK and will be discussed in detail. Other statutes which give access to personal data are the Consumer Credit Act of 1974 (to files of credit reference agencies), the Access to Medical Reports Act of 1998 and the Access to Health Records Act of 1990.[34] Where relevant, reference will be made to these Acts. Discussion of the DP Act of 1998 is preceded by a brief discussion of the legislative history of data protection legislation in the UK.

---

29 HR Act of 1998 s 3(1).

30 HR Act of 1998 s 4.

31 HR Act of 1998 s 4(6).

32 A Minister may also, in a "fast track" procedure (see Fenwick *Civil liberties* 621) amend the offending legislation by order (HR Act of 1998 s 10).

33 Jay & Hamilton *Data protection* 17. For a discussion of the impact of the Human Rights Act on the Data Protection law, see Bainbridge *Data protection law* 140–142.

34 See House of Commons Library *Research paper 98/48* 11; and see Cowley *Access to medical records and reports* for a discussion of these Acts.

4.2 Background and legislative history of Data Protection Act

4.2.1 Data Protection Act of 1984

4.2.1.1 Introduction

The first Data Protection Act of 1984 was adopted in response to both domestic and international pressure on the government to do so. Domestic pressure was exerted by different groups of people, for example the National Council for Civil Liberties, which was concerned about the threat posed to privacy by the increased used of computers to store information.

Apart from those who wanted legislation because of a concern for civil liberties, there were also parties wanting legislation for more mundane economic reasons: in order for the data processing industry in the UK to participate freely in the European market, the UK had to adopt the Council of Europe Convention on Data Protection.[35] This Convention allows signatory states to prohibit the flow of personal information to non-signatory states whose domestic law does not adequately protect the privacy of individuals when computerised processing of data takes place.[36] However, before the UK could ratify the Convention, it had to adopt data protection legislation. Economic concerns arose as a result of international pressure.[37]

The Data Protection Act of 1984 was preceded by several private members' bills and committee reports on the issue of data protection.[38] These early initiatives remain relevant because many of the

35 Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data Strasbourg 28 Jan 1981 No 108/1981 (hereafter: Convention 108/1981). See ch 3 par 3.

36 Convention 108/1981 a 12(3)(b).

37 Campbell *Data transmission and privacy* 107; Evans & Korn *Data Protection Act* 2; Savage & Edwards *Data Protection Act* 9.

38 The first Data Protection Act had a very long legislative history. Several attempts at introducing legislation were thwarted as much by elections and new governments coming to power as by unwillingness on the part of incumbent governments to effect change in this area.

principles emphasised in them still characterise current UK data protection legislation.

4.2.1.2 Private members' Bills

Since the sixties, several private members' bills have been introduced in the British Parliament on the subject of privacy, but none of them has reached the statute book.[39] The debate in Britain about computers and privacy also dates from the late 1960s. By 1969 computerisation in Britain was present on a "modest" scale,[40] but concerns were already being raised about the ever- increasing role of computers in society.[41] Plans for a centralised data bank (the Driver and Vehicle Licensing Centre) and the 1970 census emphasised these concerns among the general public.[42] Pressure groups such as the National Council for Civil Liberties and the National Computing Centre also put pressure on successive UK governments to introduce data protection legislation.[43] In 1969 and 1971 private members' Bills on data surveillance and personal information were again unsuccessfully introduced in Parliament.[44]

In 1967 a committee called "Justice"[45] was set up to examine the whole subject of privacy. It concluded that the right to privacy reflects a fundamental human need which must be respected and protected by law, that infringements of privacy will increase in any technological society, and that English law falls short of providing an adequate degree of protection of privacy. It recommended that a civil remedy

39 1972 *Int Soc Sci J* 459.

40 *Sunday Times* 2 March 1969 quoted in Warner & Stone *Data bank society* 102.

41 See eg Warner & Stone's *Data bank society* published in this period.

42 Bennett *Regulating privacy* 47 52.

43 Simons *Privacy in the computer age* 55.

44 In 1969 a private members' Bill, the Data Surveillance Bill, was unsuccessfully introduced by Kenneth Baker in the Commons and by Lord Windlesham in the Lords. This Bill called for registration of and a code of conduct for computerised personal data banks. Equally unsuccessful was the Control of Personal Information Bill introduced by Leslie Huckfield in 1971.

45 The British section of the International Commission of Jurists (Bennett *Regulating privacy* 24).

should be provided for substantial and unreasonable infringement of any person's privacy.[46]

Brian Walden introduced a draft Bill prepared by Justice late in 1969 in the House of Commons. The Bill was so popular that it reached a second-reading debate.[47] Walden withdrew the Bill when the Labour government of the time promised to appoint a committee to study the issue.[48] The committee was appointed in May 1970, a month before the Labour government fell in the general elections. Sir Kenneth Younger was appointed chairman.

4.2.1.3 Younger Committee

The Younger Committee on Privacy[49] was instructed to consider whether legislation was needed to give further protection to the individual citizen and to commercial and industrial interests against the invasion of privacy by private persons and organisations, or by companies, and to make recommendations.[50]

The Committee was therefore not permitted to consider possible invasion of privacy by government. Requests to the Labour government as well as to the new Conservative government to extend its terms of reference to include threats to privacy by government were refused. Neither was there specific reference to computers in the terms of reference of the Committee.[51]

Despite this, the Younger Committee pointed out in its 1972 report that many of the anxieties which had led to a demand for the creation of a legal right to privacy concerned the activities of the government

46 Justice *Privacy and the law* 41.

47 Brian Walden HC Debs 5s 23 January 1970 col 862-68 (quoted in Bennett *Regulating privacy* 84).

48 It was the first time that the issue was debated in Britain, and there was considerable support in the House for a statute protecting privacy. However, the Labour government of the time was ambivalent. Its intention was to block the Bill at all costs, but because it did not want to be seen as being opposed to the protection of privacy, it struck a deal with Walden (see Bennett *Regulating privacy* 85).

49 Cmnd 5012.

50 UK Home Office *Report of the Committee on Privacy* 1.

51 Madgwick & Smythe *The invasion of privacy* 15 (quoted in Bennett *Regulating privacy* 86 fn 104).

and public agencies.[52]

Despite the absence of any reference to computers in its terms of reference, the Younger Committee devoted a chapter to the threat posed to privacy by the computer. In this, it took note of previous bills on the subject of computers and privacy.[53] However, in the end the Committee was not convinced that the computer as such was a threat to privacy in the private sector, concluding that "the computer problem" as it affects privacy in Great Britain was one of apprehensions and fears and not so far one of facts and figures.[54]

However, the Younger Committee did identify three key dangers of the use of computers, namely:

- the capability of the computer to collect large amounts of data about individuals, to link, manipulate and process these and thereby to create detailed personal files
- the possibility that information about individuals could be correlated from a variety of sources
- the possibility that data held on a computer could be accessed from remote terminals[55]

The Committee proposed a set of ten principles to be observed by those holding personal information on computers, in order to prevent these potential dangers from being realised. These principles were later called the Younger principles.[56] The influence of these principles on both the data protection Acts

52 UK Home Office *Report of the Committee on Privacy* par 3 (quoted in UK Home Office *Report of the Committee on Data Protection* 4).

53 The Data Surveillance Bill of 1969 and the Control of Personal Information Bill of 1971 referred to above (see fn 44).

54 UK Home Office *Report of the Committee on Privacy* 179 (as quoted in Bennett *Regulating privacy* 86).

55 UK Home Office *Report of the Committee on Privacy* par 582 (as quoted in Lloyd *Information technology law* 39).

56 See eg UK Home Office *Report of the Committee on Data Protection* 460.

that were eventually adopted is evident in the data protection principles contained in these Acts.[57]

These principles are:[58]

- Information should be regarded as being held for a specific purpose so that it may not be used, without appropriate authorisation, for other purposes.

- Access to information should be confined to those authorised to have access for the purpose for which the information was supplied.

- The amount of information collected and held should be the minimum necessary for the achievement of a specified purpose.

- Where computerised systems handle information for statistical purposes, the design of the systems and the programs used should make adequate provision for separating identities from the rest of the data.

- There should be arrangements for informing subjects about the information held concerning them.

- The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information.

- A monitoring system should be provided to facilitate the detection of any violation of the security system.

57 See par 4.3.4.

58 See UK Home Office *Report of the Committee on Privacy* para 592 to 599 (as quoted in UK Home Office *Report of the Committee on Data Protection* 460 and Lloyd *Information technology law* 39).

- In the design of information systems, periods should be specified beyond which the information should not be retained.

- Data held should be accurate and there should be machinery for the correction of inaccuracies and the updating of information.

- Care should be taken in coding value judgements.

The Committee also pointed out the need to establish machinery to ensure the observance of these principles, but rejected both the introduction of a system of self-regulation and an institutionally based supervisory scheme, which were initially proposed in earlier Bills. It further recommended that the government should legislate to provide itself with machinery for keeping abreast of the growth in and techniques for the computer-assisted gathering and processing of personal information.[59]

This Standing Committee (as the Younger Committee referred to it) should collect information about computerised information stores and the practices followed regarding computerised information and should propose further legislation if necessary.[60]

Some recommendations of the Younger Committee were incorporated in the Consumer Credit Act of 1974. The British Computer Society also adopted some of the recommendations in a professional code of conduct.[61]

The report of the Younger Committee was debated in Parliament in 1973. The government avoided any immediate response. Instead it announced the publication of a White Paper which would set out

59 UK Home Office *Report of the Committee on Privacy* par 621 (as quoted in UK Home Office *Report of the Committee on Data Protection* 5).

60 UK Home Office *Report of the Committee on Privacy* par 621 (as quoted in UK Home Office *Report of the Committee on Data Protection* 4 and Lloyd *Information technology law* 39).

61 See Bennett *Regulating privacy* 87 fn 107.

its response to the Younger Committee's recommendations.[62] However, the Conservative government left office in 1974, and it was left to the incoming Labour administration to go on with the White Paper.

This White Paper[63] and its Supplement[64] were published two years later in 1975. According to Bennett, it reflects an important change in official thinking. Because it was difficult to muster sufficiently strong support for the recognition of a general right to privacy, from now on the issue was confined to computers and privacy (that is, data protection).[65]

On the one hand the White Paper found that there was no evidence that computers were being improperly used in the public sector, but also recognised that the risk posed by computers and the unease of the public in this regard were reason for concern. It therefore admitted that computer users can no longer be the sole judges of the adequacy of protection their systems provide to privacy of persons and concluded that the time for legislation had come.[66]

The White Paper also announced the establishment of yet another committee, the Data Protection Committee, under the chairmanship of Sir Norman Lindop.[67]

4.2.1.4 Lindop Committee

The Lindop Committee was to make recommendations as to the scope and extent of data protection

62 Lloyd *Information technology law* 40.

63 UK Home Office *Computers and privacy* Cmnd 6353.

64 UK Home Office *Computers: safeguards for privacy* Cmnd 6354. The supplement published details for the first time about categories of information likely to be held in the computer systems of government departments (*Report of the Committee on Data Protection* 6).

65 Bennett *Regulating privacy* 88.

66 UK Home Office *Computers and privacy* 3 (as quoted in Bennett *Regulating privacy* 88).

67 Initially Sir Kenneth Younger would once again have been the chairman, but he died before the appointment of all the members of the Committee (UK Home Office *Report of the Committee on Data Protection* 3).

legislation and as to the form of the supervisory mechanism which should be established.[68] Its task was to "flesh out" the White Paper which provided the skeleton of the Government's policy, namely to have legislation to create a permanent Data Protection Authority which could ensure that legal standards for safeguarding privacy were applied to computers handling personal information in both the public and the private sectors.[69]

This Committee reported in 1978.[70] The report was a comprehensive and detailed study of the impact of data processing upon individuals' rights in the UK at that time.[71] The Committee proposed legislation in terms of which all persons in the UK who use computers to handle personal information should register.[72] Such legislation should cover both the private and the public sectors. The legislation should declare a set of seven principles and establish a Data Protection Authority to implement them. The principles should be designed in the interests of the data subjects, the users and the community at large.

A feature of the report was its emphasis on flexibility: it was clearly spelled out that a single set of rules to govern all handling of personal data by computers simply would not do. The legislation would have to provide a means of finding appropriate balances between all legitimate interests. The scheme of regulation therefore had to be a flexible one: flexible enough to make allowances for different cases, different times and different interests.[73]

To achieve the desired flexibility, different Codes of Practice should be drawn up for different classes of personal data handling applications. The Codes of Practice should prescribe fair information principles and should be promulgated by statutory instruments giving them the force of law. Failure to

68 UK Home Office *Report of the Committee on Data Protection* 6–7; Lloyd *Information technology law* 41.

69 UK Home Office *Report of the Committee on Data Protection* 6.

70 UK Home Office *Report of the Committee on Data Protection* Cmnd 7341.

71 Bennett *Regulating privacy* 14.

72 The licensing system used by the Swedes was rejected as too bureaucratic (UK Home Office *Report of the Committee on Data Protection* 168).

73 UK Home Office *Report of the Committee on Data Protection* xx.

comply with the codes should result in the incurring of criminal penalties.[74] The Data Protection Authority could modify these Codes of Practice if reasonably required to do so and should be open and approachable at all times. The Data Protection Authority should be an independent,[75] multimembered authority governed by a group of people who are broadly representative of the community at large.[76] Apart from its duty to draw up and enforce the Codes of Practice, the Data Protection Authority should maintain a register of personal data applications and investigate complaints.[77]

According to one commentator the report received a lukewarm reception from government and was largely ignored in the end.[78] Another commentator is of the opinion that the report was well received, but that its publication was ill timed, since the Labour government was defeated six months later after a successful vote of no confidence.[79] In the end it was Mrs Thatcher's Conservative administration who passed the first Data Protection Act in 1984.

Many commentators argue, however, that had it not been for pressing economic arguments resulting from international pressure to adopt data protection legislation, the Data Protection Act of 1984 would not have been passed.[80]

4.2.1.5 Council of Europe Convention on data protection

74 UK Home Office *Report of the Committee on Data Protection* xxi.

75 However, the Data Protection Authority should be subject to supervision by the Council of Tribunal, the courts, and the Parliamentary Commissioner for Administration, and should report to Parliament (*Report of the Committee on Data Protection* 182 192).

76 UK Home Office *Report of the Committee on Data Protection* 185-186.

77 UK Home Office *Report of the Committee on Data Protection* 175.

78 Lloyd *Information technology law* 42.

79 Bennett *Regulating privacy* 89.

80 Bennett *Regulating privacy* 91, 141–142, 235, 236; Price "UK data protection law" 131; Simitis "New trends" 19–20.

According to Bennett,[81] the Conservative government viewed the Lindop Committee as a "Labour inspired" group. It was also distrustful of any efforts to establish another quasi-autonomous nongovernmental organisation.[82] The Lindop Committee report was thus ignored.[83] However, many other European countries had already introduced data protection laws,[84] and this movement influenced the Council of Europe to adopt the Convention for the Protection of Individuals with regard to the Automatic Processing of Data in 1981.[85] The European Commission requested the member states of the Community to sign the Convention and ratify it before the end of 1982. The European Parliament also adopted a resolution in March 1982 calling for ratification.[86]

All this placed increased pressure on the UK government, which signed the Convention in 1981. The Department of Trade and Industry was especially concerned that personal data protection could become a pretext for other European countries to legally impose trade barriers against the UK. This would lead to the isolation of the British data processing industry and other service sectors that relied on unimpeded communications.[87] Although it had signed the Convention, the UK could not ratify it unless it had its own data protection legislation. Consequently, the Conservative government had no choice but to adopt legislation.

4.2.1.6 Passage of the Data Protection Act of 1984

In April 1982 the government at long last published its proposals for legislation in another White

81 Bennett *Regulating privacy* 186.

82 Also called "quangos". It was perceived that Mrs Thatcher's mandate was to reduce the number of such organisations (Bennett *Regulating privacy* 186).

83 Rumbelow 1984 *Int Bus L'yer* 154.

84 Eg Austria (1978), Denmark (1978), France (1978), the Federal Republic of Germany (1977), Luxembourg (1979), Norway (1978) and Sweden (1977).

85 See ch 3 par 3.

86 Mellors & Pollitt 1984 *Pol Q* 311; Rumbelow 1984 *Int Bus L'yer* 154.

87 Bennett *Regulating privacy* 141–142; see also Lloyd *Information technology law* 42; Michael 1982 *Pub L* 360, 361.

Paper.[88] The Government's approach was much less rigorous than the approach adopted by the Lindop Commission.[89] Instead of a Data Protection Authority, the White Paper proposed that a single Data Protection Registrar be appointed. The Registrar would be independent of the government and responsible for overseeing a public register of computer systems that process personal data. Registered users have to comply with a general set of fair information principles. The idea of Codes of Practice was rejected because it would impose too great a burden on resources and take too much time to develop for the whole field of personal data systems.[90] The government did agree to impose a general duty on the Registrar to encourage trade associations and other representative bodies to prepare and disseminate to their members Codes of Practice for guidance in complying with the data protection principles.[91]

A Bill implementing the White Paper proposals, was introduced in December 1982, but its passage through Parliament did not take place until 1983.[92] In 1984[93] the Data Protection Act of 1984 received Royal Assent. The Data Protection Act did not become fully operational all at once. Its provisions were phased in over a period of five years. However, after five years, the UK had to prepare a new Data Protection Act to give effect to the provisions of the European Union Directive on data protection.

88 UK Home Office *Data protection: the Government's proposals* Cmnd 8539. The White Paper was produced in a hurry, after Mrs Thatcher unexpectedly announced in Parliament in February of that year that it was the Government's intention to legislate on this topic in the next Parliamentary session (Bennett *Regulating privacy* 92).

89 Savage & Edwards 1985 (6) *Computer/L J* 143 146.

90 Savage & Edwards *Data Protection Act* 11–12. There was also a constitutional argument, namely that delegated legislation of this sort should be presented by a Minister, able to take Ministerial responsibility (Michael 1982 *Pub L* 362; Samuels & Pearce 1984 *Solicitor's J* 588).

91 Savage & Edwards 1985 (6) *Computer/L J* 143 146.

92 Bennett *Regulating privacy* 92.

93 The year of Orwell's book and 23 years after the first privacy legislation was introduced (Bennett *Regulating privacy* 93).

4.2.1.7 Content of the Data Protection Act of 1984[94]

The 1984 Act reflected the work carried out by the Younger and Lindop Committees. It also drew on the OECD Guidelines and the Council of Europe Convention. It set out eight principles for data handling, largely drawn from the two international instruments and it included the concept of mandatory registration of data users advanced by the Lindop Committee. It also provided for exemptions from registration. All data users who were not exempt were required to register with the Data Protection Registrar.

In one aspect the Act did not reflect its origin: the Act was silent on the importance of the protection of privacy. The Younger and Lindop reports emphasised that the need for legislation had arisen because of the loss of personal privacy in the computer age. The international documents had also come into being about because of the importance of the protection of the right to private life. However, the 1984 Act made no reference to privacy.[95]

In the end the Act was not as effective in protecting data privacy as had been expected.[96] Some significant problems emerged in the period the Act was in force. A key problem was that only registered data users were subject to the data protection principles. This created the anomalous situation that users who failed to register, even though they were supposed to, could not be required to comply with the principles.[97] Failure by data users to register could only result in action by the Registrar for non-registration, but the principles could not be enforced against such users. Another problem area was that the subject access provision was used in an unforseen way by third parties. Data subjects were required by third parties to make subject access requests for the benefit of the third party. For instance, employers would require employees to make subject access requests to establish whether they had

94 See Jay & Hamilton *Data protection* 7–8; Aldhouse "UK Data Protection" 180–187.

95 A similar "obscure refusal to acknowledge its privacy roots" is evident in the 1998 Act (see Jay & Hamilton *Data protection* 8).

96 Charlesworth 1999 *Gov Inf Q* 203, 208

97 Charlesworth 1999 *Gov Inf Q* 203, 208. In the 1998 Act this situation has been remedied. See par 4.3.4.1.

convictions against them.[98] Another problem arose as a result of judicial interpretation of the word "use". The House of Lords held that the display of information on a computer screen did not amount to the use of such information.[99] This interpretation severely limited the Act's use in preventing "data browsing" and left what Charlesworth describes as "a key area of personal data privacy" effectively untouched by the data protection legislation.[100]

Despite these apparent problems, no major amendments to the 1984 Act were attempted and the 1998 Act came about because of the need to implement the European Union Directive on data protection in UK law.[101]

4.2.2 European Union Directive on data protection

As was mentioned previously, the European Parliament and the Council adopted a Directive on data protection in 1995 which gave member countries three years to incorporate its terms into national legislation.[102] In the UK, the implementation process began in 1996 with the publication by the Conservative government of a Consultation Paper which sought views on the way in which the Directive should be implemented.[103] The Government's position was that it intended to implement the Directive in such a way that it minimised the burden on businesses. It consequently intended to go no further than was absolutely necessary to meet its obligations under European Law, and one of the initial suggestions

98 The 1998 Act makes enforced subject access an offence (see par 4.3.10.2).

99 *R v Brown* [1996] 1 All ER 545. There was relatively little case law under the 1984 Act. *R v Brown* was the only House of Lords case that was heard. There have been four High Court cases, but not all of them have been reported.

100 Charlesworth 1999 *Gov Inf Q* 203, 210. The 1998 Act broadens the definition of "processing" to eliminate this type of interpretation. See par 4.3.3.1c.

101 Charlesworth 1999 *Gov Inf Q* 203, 210.

102 Ch 3 par 4.1.

103 UK Home Office *Consultation paper on the EC Data Protection Directive* (1996).

was that the Directive's requirements could be met by simply amending the 1984 Act.[104]

The Registrar, as well as other institutions,[105] saw this proposal as a minimalist approach to a crucial task.[106] The Registrar, Mrs Elizabeth France,[107] took the view that the most secure way of implementing the Directive was to introduce a new Bill in Parliament,[108] and in her full response to the Government's consultation paper she expressed the opinion that this was an opportunity to take a fundamental look at the way data protection operated in the UK.[109]

After the 1997 elections Mr Blair's new Labour government decided in favour of the view maintained by the Registrar. In order to meet the deadline for the implementation of the Directive, the new government was required to produce a new Act in a very short time. Detailed government proposals for new data protection legislation were published in 1997. The Data Protection Bill was debated in Parliament in the course of 1998 and received the Royal Assent on 16 July 1998.[110] However, since regulations to bring it into force had to be passed, the only provisions which immediately came into force were those dealing with definitions and giving the relevant Minister the power to draft regulations.[111] The rest of the provisions came into effect on 1 March 2000.[112]

---

104 Charlesworth 1999 *Gov Inf Q* 203, 212.

105 Such as the British Computer Society Data Protection Committee, the Campaign for Freedom of Information and UCISA (referred to by Charlesworth 1999 *Gov Inf Q* 203, 212 note 52).

106 See Ustaran & Johnson 1997(3) *JILT* 2.

107 Mrs France was the second Data Protection Registrar. The first Registrar was Mr Eric Howe. On 31 January 2001, Mrs France became the first Information Commissioner. The Information Commissioner is responsible for enforcing both the Data Protection Act of 1998 and the Freedom of Information Act of 2000. Mr Richard Thomas took up the position of Information Commissioner in December 2002.

108 DPR *Questions to answers*.

109 DPR *Our answers.* All documents of the Office of the DPR (or Commissioner), are available on its website: http://www.dataprotection.gov.uk/ under the heading "New Data Protection Law" (full address: http://www.dataprotection.gov.uk/eurotalk.htm).

110 Charlesworth 1999 *Gov Inf Q* 203, 213.

111 Although the Act missed the 24 October 1988 deadline set by the Directive, the date still remains relevant for the transitional arrangements in the DP Act of 1998. All processing of new data which started after the

(continued...)

4.3 Provisions of Data Protection Act of 1998[113]

4.3.1 Overview of structure of Data Protection Act

The DP Act is a complicated and lengthy piece of legislation. It is divided into six parts, comprising seventy-five sections, and it also has sixteen schedules.

The six parts deal with the following:

- ❒ Preliminary issues (basic interpretative provisions, sensitive personal data, the special purposes, the data protection principles, application of the Act, the Commissioner and the Tribunal – sections 1–6)
- ❒ Rights of data subjects and others (sections 7–15)
- ❒ Notification by data controllers (sections 16–26)
- ❒ Exemptions (sections 27–39)
- ❒ Enforcement (sections 40–50)
- ❒ Miscellaneous and general (sections 51–75)

The sixteen schedules deal with the following:

- ❒ the data protection principles
- ❒ conditions relevant for the purposes of the first principle: processing of any personal data
- ❒ conditions relevant for the purposes of the first principle: processing of sensitive personal data

111(...continued)
24 October 1998 deadline immediately had to comply with all the provisions of the DP Act of 1998 once it came into force. Any processing which was already under way before the deadline has 3 years from that date in which to comply, ie until 24 October 2001. During that period processing already under way on 24 October 1998 will effectively only have to comply with the 1984 Act (see DPR *Advice on new law* 1). In this thesis the transitional provisions will not be discussed in any detail, but note that until at least 23 October 2001 there were dual regimes in force (see Chalton et al *Encyclopedia of data protection* par 1– 075).

112 See DPR *1998 Data protection law: latest update*.

113 The DP Act is not accompanied by an explanatory document or memorandum, as eg the Netherlands WBP is, which makes it difficult to give a full explanation of all of provisions. The intention of the legislature has to be gathered from the Parliamentary debates or consultation papers preceding the adoption of the Act. See also Jay & Hamilton *Data protection* 8–9.

- ❒ cases where the eighth principle does not apply
- ❒ the Data Protection Commissioner and the Data Protection Tribunal
- ❒ appeal proceedings
- ❒ miscellaneous exemptions
- ❒ transitional relief
- ❒ powers of entry and inspection
- ❒ further provisions relating to assistance under section 53
- ❒ educational records
- ❒ accessible public records
- ❒ modifications of the Act having effect before 24 October 2007
- ❒ transitional provisions and savings
- ❒ minor and consequential amendments
- ❒ repeals and revocations

4.3.2 Purpose of Data Protection Act

The DP Act of 1998 is described in its title as

> ...an Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

In other words, the purpose of the DP Act of 1998 is to regulate the processing of information in a new manner and, as we have seen, the methods introduced have to satisfy the European Union Directive on data protection.[114] However, despite the clear provisions in the Directive relating to private life, the DP Act makes no mention of the protection of privacy as a purpose of the Act. Like the 1984 Act, the

114 See Slee 1999 *Inf & Comm Tech L* 71–109 for a comparative examination of the Data Protection Bill 1998 and the EU Directive on data protection.

1998 Act refuses to acknowledge its privacy roots.[115]

4.3.3 Scope of application of Data Protection Act

Two aspects are considered here: the scope of the DP Act as determined by the definitional framework of the Act and the scope of the DP Act as it relates to territorial application.

4.3.3.1 Definitional framework

The DP Act regulates the **processing** of **personal data** on **data subjects** by **data controllers** or **data processors**.[116] No distinction is made between processing of data in the **private** or **public sectors**, and the DP Act applies equally to both areas.

a Data

The definition of "data" is an important part of many of the other definitions in the DP Act and in effect limits the application of the DP Act of 1998, since the Act is only applicable if the personal information involved complies with the definition of data. It should also be noted that the Act draws a clear distinction between the concepts "data" and "information". Data are defined[117] as information which is either processed in a certain way, or recorded[118] in a certain way.

First of all, data consists of information that is processed by means of equipment which operates automatically in response to instructions given for that purpose. In other words, in this case the information is in a form capable of being processed by computer equipment. Examples would include

115 Jay & Hamilton *Data protection* 8.

116 Singleton *Data protection* 1.

117 In DP Act of 1998 s 1(1).

118 "Recorded" is not defined, but presumably includes manuscript, audio, analogue, digital, transient, electronic and photographic recording (see Chalton et al *Encyclopedia of data protection* par 1-063/1).

most computer files, word processors, database software, and spreadsheets.[119] Secondly, data are also information recorded with the intention that its processing should take place by means of such equipment.[120] Examples include information collected from registration forms, fingerprints collected on paper with the intent of scanning them into a database, and closed circuit television pictures.[121] These provisions clearly relate to the automatic processing of information.[122]

However, data also include information recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system. A "relevant filing system" is defined as meaning any set of information relating to individuals (in other words natural persons) to the extent that, although the information is not processed automatically, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.[123] This provision has the effect of including manually processed information or paper-based information in the definition of data (provided of course that the information is readily accessible because it forms part of a filing system that is structured with reference to individuals or to criteria relating to individuals).[124] Examples of such data would include a card file

119 Charlesworth 1999 *Gov Inf Q* 203, 213.

120 It is not clear who should hold the intention or when it should be held (see Chalton et al *Encyclopedia of data protection* par 1-063/2).

121 Charlesworth 1999 *Gov Inf Q* 203, 213

122 It is evident from these provisions that the DP Act will not be applicable if a person merely possesses or holds personal data without intending to process it. However, as soon as the data is stored, they fall within the definition of "processing" (see Mullock & Leigh-Pollitt *Data Protection Act explained* 18). A definition of "data" does not appear in the Directive. The Directive applies to the processing of personal data by automatic or nonautomatic means. Personal data are broadly defined as any information relating to an identified or identifiable natural person, and processing of data equally broadly includes any operation performed upon personal data (Dir 95/46/EC a 2(a)). Under the Directive, therefore, any information that relates to an individual is personal data to which the Directive applies. The DP Act of 1998, on the other hand, is only applicable if the information that relates to an individual also falls within the definition of data, and as has been said, this means information that is processed automatically, or recorded with the intention of processing it automatically. Also see fn 151.

123 DP Act of 1998 s 1(1).

124 The DP Act of 1984 did not include manually processed information in its scope. However, the provisions of the Directive on data protection necessitate the inclusion of manual files that are structured according to specific criteria relating to individuals, allowing easy access to personal data. The provenance of the

(continued...)

structured by name, address, or Social Security number or other identifier, Rolodex, and non-automated microfiche.[125]

In preliminary guidelines on the DP Act of 1998 the Data Protection Registrar emphasises that whether or not manual files fall within the definition of "data" will be a matter of fact in each case.[126] In deciding this, data controllers should consider the following:

- There must be a set of information about individuals.[127]
- The set must be structured by one of two mechanisms – by reference to individuals themselves or by reference to criteria relating to individuals.[128]
- The structuring must work in such a way that specific information about a particular individual is readily accessible.[129]

Ultimately, data also include information that does not fall into any of the above categories, but forms

---

124(...continued)
provision in the Directive that includes manual files is the German Federal Data Protection Act (Bundesdatenschutzgesetz) of 1993 (see Jay & Hamilton *Data protection* 23). The UK was opposed to the inclusion of manual files in the scope of the Directive (see Greenleaf 1995 (2) *Int Priv Bul* 11). According to Carey *Data Protection Act 1998* 7–8 the right of access to paper-based filing systems is likely, for UK businesses, to be the most costly and time-consuming aspect of the new regime. Note that data controllers may not immediately have to comply in full with the provisions of the DP Act – certain transitional relief may apply (see DP Act of 1998 sch 8). Where it does, manual data are exempt from the data protection principles, individual rights and notification requirements until 24 October 2001.

125 Charlesworth 1999 *Gov Inf Q* 203, 214.

126 DPR *Data Protection Act 1998* 4. Also see Carey *Data Protection Act 1998* 8.

127 The word "set"suggests a grouping together of things by reference to a distinct identifier, ie a set of information with a common theme or element (DPR *Data Protection Act 1998* 4).

128 Criteria relating to individuals include aspects such as age, sickness record, type of job, credit history, shopping habits, membership of particular organisations (DPR *Data Protection Act 1998* 4).

129 According to Jay & Hamilton *Data protection* 34, when interpreting the definition of data, it should be borne in mind that the intention of the UK government was that only highly structured manual files should be included in the definition of data in the 1998 Act. The definition should not include files merely because they bear the names of individuals. According to these authors, examples of files that will be included are indexed systems, structured reports or structured files.

part of an "accessible record" as defined by the Act.[130] An accessible record is a health record,[131] an educational record[132] or an accessible public record.[133] This part of the definition of "data" was added to ensure that certain rights of access to manual records are covered under the Act. These are rights under the Personal Files Act of 1987, the Access to Health Records Act of 1990, the Education (School Records) Regulations of 1989 and corresponding legislation in Scotland and Northern Ireland. They relate to local authority housing and social services records, health records, and records held by schools on pupils and former pupils.[134]

b Personal data

Personal data are defined as data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.[135] Personal data include any expression of opinion about the individual and any indication of the intention of the data controller or any other person in respect of the individual. What this means in effect is that an employer would not only have to disclose his or her opinion of an employee, but also his or her intention to fire or promote an employee as a result of the

130 DP Act of 1998 s 68(1).

131 As defined in the DP Act of 1998 s 68(2).

132 As defined in the DP Act of 1998 sch 11.

133 As defined in DP Act of 1998 sch 12.

134 Singleton *Data protection* 2. The inclusion of "accessible record" in the 1998 Act arose from concern on the part of the government to establish a statutory basis for rules reflecting the judgment of the European Court of Human Rights in *Gaskin v United Kingdom* [1989] 12 ECHR 36 (see Chalton et al *Encyclopedia of data protection* par 1-063/2; Singleton *Data protection* 2). This case required that access should be given to the data subjects of these types of records, but also held that it is acceptable that the public interest in preserving the confidence of those who have contributed to the record, should be balanced against the subject's right of access. The justification for such a rule was preservation of confidence so as to ensure frankness in disclosing sensitive information and opinions.

135 According to Charlesworth 1999 *Gov InfQ* 203, 214 this means that data controllers will have to be aware of the long-term ramifications of data collection strategies.

opinion, to give one example.[136]

From the term "individual" used in this definition it is evident that in order to be classified as personal data the data must concern a natural person. Data on juristic persons cannot be considered to be "personal data." Consequently, the DP Act of 1998, like its predecessor, does not protect data on juristic persons.[137]

The data must also relate to a living individual. The Directive does not make it clear whether natural persons include dead persons, and some commentators argued that the term "natural persons" could do so.[138] However, the DP Act of 1998 clearly refers to living persons only.[139]

According to the definition, the data should "relate" to a living individual. The concept of "relating" to an individual is very broad. In general, there is no exclusivity about data and the same data can relate to more than one person.[140] Personal data are also not limited to private or family data; data can relate

136 See Charlesworth 1999 *Gov Inf Q* 203, 214. The DP Act of 1984 excluded "indications of intention" from the definition of personal data. In practice it proved to be problematic to make a distinction between "expressions of opinion" and "indications of intention". See also Lloyd *Information technology law* 61; Nugter *Transborder flow of personal data* 116. Dir 95/46/EC does not make such a distinction. According to Chalton et al *Encyclopedia of data protection* par 1-066/2 new exemptions given under the 1998 Act for confidential references, management forecasts and records of negotiating intentions of data controllers may have the effect in some cases of restoring, at least in part, the effect of the 1984 Act's exclusion of intentions from the definition of personal data. Also see Chalton 1997 *Computer L & Sec Rep* 425–426. See par 4.3.6.3 for the exemptions.

137 This is also the case in the Directive (see Dir 95/46/EC a 2(a)).

138 See Pounder & Kosten 1995 (21) *Data Protection News* 6. They point out that genetic profiling may justify protecting information on dead persons, because the use of data concerning a deceased person can have repercussions for living relatives.

139 The Act follows the principle in English law that persons lose all of their rights when they die – eg the estate of a dead person cannot bring an action for libel or slander (see Singleton *Data protection* 2). Note, however, that Chalton et al *Encyclopedia of data protection* par 1– 067 argue that it is not beyond doubt that deceased persons cannot be data subjects under the Act, because the Act's definition of "data subject" has no reference to living individuals. They argue that a deceased individual can be the subject of personal data which also relate to a living individual, so qualifying those data as personal data under the 1998 Act's definition of that term. However, the government intended to limit the application of the Act to living individuals (see Chalton 1997 *Computer L & Sec Rep* 425).

140 Eg where two persons hold a joint bank account, the personal data will relate to both of them (see Jay & (continued...)

to individuals' business lives, professional lives or private lives.[141]

The definition of personal data also includes data consisting of information which by itself does not identify an individual, but which combined with other information in the possession of the data controller, or which is likely to come into the controller's possession, is sufficient to provide an identification.[142] For example, where data are encrypted, but the controller is in possession of the key, or likely to come into possession of it, the data will also be personal data.[143]

The ability to identify the individual from the data is an important aspect of the definition of personal data, since the premise underlying data protection is that the processing of data relating to individuals constitutes a threat to the individuals' right to privacy. If an individual cannot be identified from the manner in which data are processed, there can be no significant threat to privacy and no justification for the application of legislative controls.[144] There is a difference between the DP Act and the Directive in this regard: In the context of the Directive,[145] information about both "identifiable" and "identified" persons is personal data, whereas the Act only refers to "identified" persons.[146] It is unclear why a more

140(...continued)
Hamilton *Data protection* 29).

141 Jay & Hamilton *Data protection* 29.

142 Chalton et al *Encyclopedia of data protection* par 1-066/2 point out that this means that data may be personal data even though the data controller may not yet be aware of the existence of the data subject and may not have any current means of identification. According to them this test of the likelihood of future possession of identifying information will be difficult to apply.

143 Carey *Data Protection Act 1998* 9.

144 Lloyd *Data Protection Act 1998* 18. Also see ch 5 par 4.3.3.1.a on this issue.

145 Dir 95/46/EC a 2(a). See ch 3 par 4.2.3.

146 Jay & Hamilton *Data protection* 29–30 explain that "someone is identifiable if their identity can be ascertained from the information held plus the result of reasonable enquiries, whether made by the controller or another. For example, if an individual's sex, height and fingerprints are held by a store detective on a file, the question of whether that person can be identified may depend upon whether police records show those fingerprints and other identifiable particulars, including possibly a name, address and description. The question of whether the data in the hands of the store detective are personal data does not [in the Directive] depend on the knowledge of the store detective or of the likelihood of disclosure by the police. In the Directive, the question of identification is left at large. In the UK Act, however, it has been
(continued...)

restrictive approach has been adopted.[147]

The Directive applies to sound and image data.[148] During the Parliamentary debate on the DP Act of 1998 the government also made it clear that it considered processing by means of closed circuit television (CCTV) and other related systems to fall under the terms of the Act.[149] Sound and image data are therefore also personal data under the DP Act of 1998, provided such data are processed by automatic means (in other words by a computer) or recorded with the intention that they should be processed automatically – only then will such data be data as defined by the Act.[150] Lloyd points out that a person might possess many hours of video recordings, but until the intention is formed to subject these recordings to processing the Act will not apply.[151]

146(...continued)
tied either to the data itself or to the knowledge or likely knowledge of the data controller."

147 Jay & Hamilton *Data protection* 30 give an example of a case heard in the Sheriff's court in Aberdeen under the 1984 Act to illustrate the different results that would be reached under the Directive and the DP Act. In that case an airline held the names of about twenty passengers together with the details of their flights. The data did not include addresses, photographs or descriptions. The question for the Sheriff was whether that list of names was personal data, ie was it information from which a living individual could be identified? The prosecution argued that it was, but the Sheriff dismissed the case on the basis that this was incorrect, reasoning that the airline could not distinguish individual passengers from one another merely by their names and therefore could not identify each passenger uniquely. According to Jay & Hamilton, there is no doubt that if the definition of personal data in the Directive were applied to such data the data would be found to be covered. However, if the definition in the 1998 Act is adopted, it could give rise to arguments like the one in the Aberdeen case. These authors feel, however, "that in the end, an interpretation consistent with the Directive would have to prevail." Another example to illustrate the importance of this difference is the fact that e-mail addresses can sometimes identify an individual, but sometimes more information is needed to make the identification. Under the Directive e-mail addresses will always be personal data, but under the DP Act there will be some e-mail addresses that will not qualify. However, the Commissioner has advised that all e-mail addresses should be considered to be personal data (see also Carey *Data Protection in the UK* 143–144).

148 Dir 95/46/EC recital 14.

149 Singleton *Data protection* 6.

150 See fn 122. On the applicability of the Data Protection Act on CCTV, see Carey *Data Protection in the UK* 148 *et seq*. See also Bainbridge *Data protection law* 130.

151 Lloyd *Data Protection Act 1998* 16. It is suggested that this is not the correct approach. The recording of personal information already constitutes infringement of the privacy of individuals. Why should it be permissible to make video recordings of individuals without this falling under the provisions of the Act requiring a lawful purpose for such recordings? The Directive, as has been pointed out, applies to the processing of personal information, and the recording of information is also considered to be processing.
(continued...)

c Processing of data

Processing, in relation to information or data,[152] means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- ❒ organisation, adaptation or alteration of the information or data
- ❒ retrieval, consultation or use of the information or data
- ❒ disclosure of the information or data by transmission, dissemination or otherwise making such data available
- ❒ alignment, combination, blocking, erasure or destruction of the information or data[153]

Obtaining, recording, using or disclosing personal data includes doing all of this with the information contained in the data.[154]

This definition of processing is much broader than that contained in the previous Act,[155] this amplitude having been necessitated by the provisions of the Directive.[156] This definition would appear to include anything that can be done with data.[157] The inclusion of "the retrieval, consulta

151(...continued)
This means that under the Directive a person will not be allowed to make a video recording of individuals unless grounds are present that make the processing lawful (see fn 122 and ch 3 par 4.2.3).

152 As has been pointed out (see par (a) above), the Act makes a distinction between information and data when defining data.

153 DP Act of 1998 s 1(1).

154 DP Act of 1998 s 1(2).

155 It incorporates inter alia the concepts of "obtaining', "holding" and "disclosing" which were dealt with separately in the 1984 Act. It also includes processing otherwise than by reference to the data subject, which was specifically excluded from the ambit of the 1984 Act (DPR *Data Protection Act 1998* 46).

156 The DP Act of 1984 had a specific exemption for word processing activities, which had to be forgone under the DP Act of 1998 (see Singleton*Data protection* 7). Like the definition of "personal data", the definition of "processing" has not been directly transposed from the Directive. The reasoning behind this is again obscure (Jay & Hamilton *Data protection* 30).

157 This was indeed the view of the first Data Protection Commissioner, Mrs Elizabeth France (see DPR *Data Protection Act 1998* 6; Carey *Data Protection Act 1998* 9). There has been comment that some express (continued...)

tion or use" and "disclosure ... or otherwise making available" of the information or data in the definition of processing, nullifies the distinction made by the House of Lords in *R v Brown*[158] between "use" and (what the House of Lords considered to be) "non-use" where data are displayed on a screen.[159]

It is immaterial whether the intention is that the information should be processed or should form part of a filing system only after being transferred to a country outside the European Economic Area (EEA);[160] the DP Act would still apply.[161]

d Data controller and data processor

The data controller and data processor are two of the primary players in the data protection regime under the 1998 Act. The term "data controller" is new in UK data protection law, and was inserted because of the requirements of the Directive. The definition given by the DP Act of 1998 essentially follows the wording of the Directive: A data controller means a person[162] who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any

157(...continued)
reference to data matching should have been included in the definition of processing, but according to Chalton et al *Encyclopedia of data protection* par 1-064/1 it is difficult to see how the activities necessary for data matching could be undertaken without performing one or more of the specific acts listed in the definition of processing. But see *R v Dept of Health ex p Source Informatics Ltd* [2000] 1 All ER 786 where it was held that under the Data Protection Act of 1984 and the 1995 Directive the process of anonymising data does not need to comply with the first data protection principle that data should be processed fairly and lawfully. By implication it means that the process of making data anonymous does not amount to the processing of the data. See also Rowland & Macdonald *Information technology law* 388–389.

158 [1996] 1 All ER 545 (see fn 99).

159 Charlesworth 1999 *Gov Inf Q* 203, 215.

160 The EEA consists of the fifteen European Union member states (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, UK) together with Iceland, Liechtenstein and Norway (see DPR *Data Protection Act 1998* 15; Carey *E-privacy* 132).

161 See DP Act of 1998 s 1(3). An example of this would be where someone in the UK gives personal information over the phone to someone in a third country who then enters the information on a computer (see DPR *The eighth data protection principle and TBDF* 4).

162 The Directive refers to a natural or legal person, public authority, agency or any other body. However, "person" could probably be interpreted as encompassing all these terms.

personal data are, or are to be, processed.[163]

Note that the controller has to determine both the purpose and the manner of the processing; in other words this is a cumulative requirement.[164] The purpose and manner of the processing need not be determined exclusively by one controller; this can be done "jointly" or "in common". According to the Data Protection Registrar, "jointly" refers to a situation where the determination is carried out in collaboration, whereas "in common" refers to where data controllers share a pool of information, each processing it independently from the other. The degree of control exercised by the different data controllers may vary, in that one may have more control over obtaining the data, and another may have more control over the way they are used.[165]

Where personal data are processed under any enactment, such as an Act of Parliament, and they are processed only for the purposes of the enactment, the person on whom the obligation to process the data is imposed by that enactment is the data controller for the purposes of the DP Act.[166] An employer who is required by a statutory provision to keep a record of employees' tax payments is an example of a data controller as described in this provision.[167]

A second important player under the Act is the data processor. A data processor is defined by the DP Act as any person (other than an employee of the data controller) who processes the data on behalf

163 DP Act of 1998 s 1(1). Note that a person will be a data controller with regard to particular personal data even if processing has not yet occurred, if the intent is that it will be processed. Eg, if personal data are collected from individuals via a newspaper promotion, and the person running that promotion intends to place such personal data in a computer database, the person will be a data controller at the time of collection (see Charlesworth 1999 *Gov Inf Q* 203, 214).

164 See Chalton et al *Encyclopedia of data protection* par 1-070/1.

165 DPR *Data Protection Act 1998* 6. Under the 1984 Act, the High court held in *Griffin v Data Protection Registrar* (1994) (unreported) that an accountant who processes data on behalf of a client could be a data user (now a data controller) if he or she exercised sufficient control over the contents of the data (see Jay & Hamilton *Data protection* 44).

166 DP Act of 1998 s 1(4).

167 Jay & Hamilton *Data protection* 34.

of the data controller.[168] Since employees of the data controller cannot be data processors, this means that a data processor will be a person contracted to process data, for example, an information technology company.[169] The Act imposes a higher duty of care upon data controllers when the processing of data is carried out on their behalf by data processors.[170]

e Data subject, third party and recipient

The third important player under the 1998 DP Act is the data subject. The term "data subject" refers to an individual who is the subject of personal data.[171] As has already been said, the term "individual" excludes juristic persons. Presumably, the individual must be a living individual, in view of the Act's definition of "personal data".[172]

Apart from the "three primary players" under the Act,[173] namely the data subject, the data controller and data processor, two other categories of persons are relevant in the Act, namely third parties and recipients.[174] A third party means any person other than the data subject, the data controller, or any

168 DP Act of 1998 s 1(1).

169 Charlesworth 1999 *Gov Inf Q* 203, 214–215.

170 See par 4.3.4.8 and DPR *Data Protection Act 1998* 7. A processor is similar to a computer bureau under the 1984 Act (Jay & Hamilton *Data protection* 36).

171 DP Act of 1998 s 1(1).

172 See par (b) above. Also see Charlesworth 1999 *Gov Inf Q* 203, 214 who paraphrases the definition of data subject as "any living individual who is the subject of personal data." However, see fn 139 for the viewpoint of Chalton et al *Encyclopedia of data protection* par 1– 067 that it is not beyond doubt that deceased persons cannot be data subjects under the Act, because the Act's definition of "data subject" contains no reference to living individuals.

173 See Charlesworth 1999 *Gov Inf Q* 203, 214.

174 The definition of third party is important in relation to the application of the "fair processing" code which requires notice to be given to third parties (see par 4.3.4.2). The definition of recipient is of importance in relation to the notification requirement and the subject access right. The Commissioner must be notified of the recipients to whom the data controller intends or may wish to disclose the data, and when data subjects enforce their right to access, they must be told who the recipients of their data will be (see par 4.3.7 and par 4.3.5.1).

data processor or other person authorised to process data for the data controller or processor.[175] The term "third party" only refers to those outside the ambit of the data controller's authority, and would not include an employee or an agent of the controller.[176]

A recipient of personal data is any person to whom the data are disclosed. This would include any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom data are disclosed in the course of processing the data for the data controller. However, a person to whom disclosure is made as a result of a particular inquiry by that person made in the exercise of any power conferred by law is not a recipient.[177]

It follows from the above that any person to whom personal data are disclosed is a recipient, and will also be a third party unless that person is the data subject, the data controller or processor or other person authorised to process the data for the data controller or processor in relation to those data.[178]

4.3.3.2 Territorial application of Data Protection Act

In setting out the limits of processing covered by UK law, the DP Act of 1998 follows the Directive on data protection. The general rule in the Directive is that a controller who is established in an EU member state must follow the national law applicable to the place in which he or she is established. If the controller has establishments in more than one state, the relevant national law of each place must be followed.[179]

The DP Act applies to a data controller in respect of data if the data controller is established in the UK

175 DP Act of 1998 s 70.

176 Jay & Hamilton *Data protection* 37.

177 DP Act of 1998 s 70.

178 See Chalton et al *Encyclopedia of data protection* par 1– 073/3.

179 Dir 95/46/EC a 4 and recitals par (19). See ch 3 par 4.2.6.

and the data are processed in the context of such establishment. It also applies to a data controller who is not established in the UK (or in any other EEA state for that matter), but who uses equipment in the UK for processing the data.[180] However, if the equipment is used merely for the purposes of transferring the data through the UK, the DP Act would not apply.[181] Where the controller is not established in the UK or another EEA state but uses equipment in the UK, the controller must nominate a representative established in the United Kingdom who, it is assumed, will be responsible for compliance with the Act.[182]

Since establishment is a key concept, the Act expands on the interpretation of this term. The following persons are considered to be established in the UK:

- ❒ an individual who is ordinarily resident in the United Kingdom
- ❒ a body incorporated under the law of, or of any part of, the United Kingdom
- ❒ a partnership or other unincorporated association formed under the law of any part of the United Kingdom
- ❒ any person who does not fall within one of the above, but maintains an office, branch or agency through which he carries on any activity, or a regular practice in the UK[183]

180 In other words, a data controller who is processing data in the UK, but who is not subject to the Directive. An example would be a USA corporation which has no offices or agents in the UK, but which purchased mailing lists in the UK, which it then used to mail marketing material from the USA to UK consumers (Jay & Hamilton *Data protection* 42).

181 DP Act of 1998 s 5(1). The 1984 DP Act was not applicable to data held and services provided outside the UK (see DP Act of 1984 s 39; Chalton et al *Encyclopedia of data protection* par 1– 060/18).

182 DP Act of 1998 s 5(2). The intention appears to be that the nominated person will be responsible for compliance with the Act for processing that takes place in the UK. However, the Act does not explicitly impose such a responsibility. In the Netherlands, failure to nominate a representative leads to criminal liability (see Neth chap par 4.3.3.3).

183 DP Act of 1998 s 5(3).

4.3.4 Data protection principles

4.3.4.1 Introduction

As we have seen, the Directive does not spell out a set of data protection principles as was found in previous international documents like the Council of Europe Convention or the OECD guidelines. Instead, it contains general rules on the lawfulness of data processing which translate the general principles into specific rules for data protection.[184] However, the DP Act of 1998 contains in part 1 of schedule 1 a set of eight general data protection principles, similar to those found in the previous DP Act of 1984.[185] It has been said that these principles "lie at the very root of data protection law" and that "all else flows from them".[186]

It is the duty of every data controller to comply with the data protection principles in relation to all personal data in respect of which he or she is the data controller.[187] This is different from the 1984 Act, in terms of which only registered data users were subject to the data protection principles.[188] The Commissioner has the duty to promote "the following of good practice" by data controllers and, in particular, to promote the observance of the requirements of the Act by data controllers.[189] The

184 See ch 3 par 4.2.4.

185 Although similar, the principles are not exactly the same. Eg, the DP Act of 1998 conflates the DP Act of 1984's second and third principle into a single new second principle (Chalton et al *Encyclopedia of data protection* par 1– 076). It also introduces a new eighth principle.

186 Bainbridge *Data protection law* 66.

187 DP Act of 1998 s 4(4). This obligation is subject to s 27 which exempts certain data which are covered by part IV of the Act.

188 The registration system that existed under the DP Act of 1984 was replaced with a notification system in the 1998 Act. All data controllers must comply with the Data Protection Principles, whether they are subject to the notification requirement or not (DPR *Data Protection Act 1998* 8). On the notification requirement, see par 4.3.7. Chalton et al *Encyclopedia of data protection* par 1– 077 point out that there is no direct obligation on a data processor who is not also a data controller to comply with any of the principles. The data processor will have an indirect obligation to comply with the seventh principle (security) by virtue of the statutory interpretation of the seventh principle (see text to fn 321).

189 DP Act of 1998 s 51(1). See par 4.3.9.1.

Commissioner enforces the principles by the serving of enforcement notices.[190] A breach of the data subject's rights entails a breach of the sixth principle. By enforcing their rights as data subjects, the data subjects will therefore also be enforcing the principles.[191]

The data protection principles must be interpreted in accordance with part II of schedule 1.[192] The interpretations are not exhaustive, and the Commissioner will probably make further interpretations in guidelines.[193] There are exemptions from some of the principles for personal data used for certain purposes. These exemptions will be discussed later on.[194]

4.3.4.2 First principle: fair and lawful processing

a General

The first principle requires that personal data must be processed fairly and lawfully and, in particular, must not be processed unless at least one of the conditions in schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met.

"Lawfully" is not defined by the Act, but it is clear that the minimum requirement is that conditions of schedule 2 and 3 must be complied with before the processing can be considered lawful. However, compliance with these conditions is not on its own sufficient to make processing lawful.[195] Jay and

190 See also par 4.3.8.3.

191 Jay & Hamilton *Data protection* 45–46.

192 DP Act of 1998 s 4(2).

193 Singleton *Data protection* 25.

194 See par 4.3.6.

195 According to Jay & Hamilton *Data protection* 52 the first principle requires that "personal data must be processed fairly **and** lawfully **and** in accordance with the schedule 2 and 3 preconditions. The clear implication here is that 'lawfully' means more than compliance with the 1998 Act alone."

Hamilton[196] explain that data processing may also be unlawful because of a breach of another statutory provision (for example, obtaining data by "hacking" contrary to the Computer Misuse Act of 1990) or because of breach of common law, such as of a breach of a duty of confidence, or a breach of the duty of a public authority to act within its powers (*ultra vires* rule),[197] or a breach of the duty not to breach a legitimate expectation. Information obtained in breach of a contractual agreement would also be regarded as having been obtained unlawfully.[198]

"Fairly" is also not defined by the Act, but the term is subjected to extensive interpretation in the Act.[199] The Act formulates a "fair processing code", but makes it clear that compliance with the fair processing code will not in itself ensure fair processing, although in such circumstances processing will be regarded as having been done fairly unless there is evidence to the contrary.[200]

The Data Protection Registrar has advised that fairness and lawfulness should both be tested against

196 Jay & Hamilton *Data protection* 47– 52.

197 Under the 1984 DP Act the Tribunal has held *obiter* that *ultra vires* actions and the breach of a duty of confidence would amount to unlawfulness (see *British Gas Trading Ltd v Data Protection Registrar* (1998) (unreported) as quoted in Jay & Hamilton *Data protection* 47).

198 Jay & Hamilton *Data protection* 51.

199 In *British Gas Trading Ltd v Data Protection Registrar* (1998) (unreported), British Gas appealed against an enforcement notice issued by the Data Protection Registrar under the 1984 Act. The notice claimed that British Gas unfairly processed personal data relating to their customers. A notice was sent out to customers that their information would be used for marketing purposes, only after the data had been collected. Customers could then notify British Gas that they did not wish their information to be used for such a purpose (ie, they could "opt out"). The Registrar felt that this was unfair. In the light of the fact that British Gas was a monopoly, the fair option would have been to allow customers to "opt in" rather than "opt out." The Tribunal agreed with the Registrar. Also see fn 230. In *Innovations (Mail Order) Limited v Data Protection Registrar* (1993) (unreported) it was held that personal information is not fairly obtained unless the data subject is told of the non-obvious purposes for which it will be used prior to obtaining the information (see also Rowland & Macdonald *Information technology law* 393.) Another case under the 1984 Act that also dealt with the question of fair processing was *CCN Systems Ltd and CCN Credit Systems Ltd v Data Protection Registrar* (1991) (unreported). In this case the method of processing was held to be too wide and therefore unfair – data was processed by reference to an address and not by reference to a name, resulting in persons being judged a bad credit risk on the basis of another person's record, where all that the persons had in common was that they had, at separate times, lived at the same address.

200 DPR *Data Protection Act 1998* 11.

an objective standard in which the intentions or views of the data user are not relevant.[201]

b Interpretation by Act

In interpreting the first principle, two issues are raised by the Act, namely fairness in processing data (the so-called fair processing code)[202] and compliance with specific conditions in order to make processing lawful.

i Fair processing code

The fair processing code involves fairness in obtaining the information, in providing the data subject with specific information, and regarding conditions for processing personal identifiers.

1 Fairness in obtaining data

According to the DP Act of 1989, in determining whether personal data are being processed fairly, regard should be had to the method by which they were obtained, including in particular whether any person from whom they were obtained was deceived or misled as to the purpose or purposes for which they were to be processed.[203] Data will be deemed to have been obtained fairly if they consist of information obtained from a person who was either authorised by national statute or obliged under national or international provisions to supply such data.[204] For example, information obtained directly from the electoral roll will be deemed to have been fairly obtained, as there is a statutory obligation on the electoral registration officer to make such information public.[205]

201 DPR *Guidelines* 59.

202 See DPR *Data Protection Act 1998* 11.

203 DP Act of 1998 sch 1 part II par 1(1).

204 DP Act of 1998 sch 1 part II par 1(2).

205 Jay & Hamilton *Data protection* 56; Lloyd *Data Protection Act 1998* 50.

2 Fairness in providing information to data subjects

As required by the Directive,[206] the DP Act of 1998 provides that personal data should not be treated as having been processed fairly unless, when data were obtained from the data subject, the data controller ensured as far as is practicable that the data subject had certain information,[207] or was provided with such information, or that such information was made readily available to the data subject.[208]

The information that must be supplied, referred to as the "fair processing information",[209] is the identity of the data controller, the identity of any nominated representative, the purpose or purposes for which the data are intended to be processed, and any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.[210]

Where the data were not obtained from the data subject (for example, where they were obtained from the data subject's wife or parent, or were bought from another controller[211]), the data controller must also ensure that the data subject has or has been provided with the specified information, or that such

206 Dir 95/46/EC a 10 and 11.

207 According to Jay & Hamilton *Data protection* 58 the term "has" (the word used in the Act), seems to be designed to cover a multi-stage data gathering exercise and to enable the data controller to provide the data subject with the requisite information at just one rather than at every stage.

208 DP Act of 1998 sch 1 part II par 2(1)(a). Jay & Hamilton *Data protection* 56 point out that the phrase "has been made readily available" (the words used in the Act) is open ended and ripe for different interpretations. The phrase does not appear in the 1984 Act, and will have to be interpreted anew by the Tribunal and the courts. These authors are of the opinion that if this phrase is interpreted as meaning that information might be available to the data subject only on application rather than actively provided to him or her, this interpretation will sit "very uneasily" with the requirement of informed consent (one of the conditions for lawful processing – see par ii hereunder).

209 See DPR *Data Protection Act 1998* 12.

210 DP Act of 1998 sch 1 part II par 2(3). The Data Protection Registrar advised that the more unforseen the consequences of the processing are for data subjects, the more likely it is that data controllers will be expected to provide further information (DPR *Data Protection Act 1998* 12).

211 See Jay & Hamilton *Data protection* 56.

information has been made readily available to him or her. This must be done before "the relevant time" or as soon as practicable after that time.[212]

The definition of "relevant time" is a complex one, but in essence it means that when a data controller plans to keep data for himself or herself, the "relevant time" when the data subject has to be provided with the required information is when processing first takes place. However, if the data controller is planning to disclose the data to a third party, the relevant time is when that disclosure first takes place. If the data controller originally plans to disclose to a third party but then changes his or her mind, then the relevant time is when the data controller changes his or her mind.[213]

However, the controller need not give the information to the data subject before the relevant time where the provision of such information would involve a disproportionate effort, or where the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract. The Secretary of State may prescribe further conditions which must be met before the controller will be exempted from giving the information.[214]

"Disproportionate effort" is a new phrase which will be subject to different interpretations. According to the Directive, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.[215] Carey suggests that "disproportionate effort" relates to the consequence of the activity for the data subject. Where the effort needed to contact the data subject is considerable, this is likely to constitute a disproportionate effort, unless it is outweighed by the

212 DP Act of 1998 sch 1 part II par 2(1)(b).

213 DP Act of 1998 sch 1 part II par 2(2). See also Jay & Hamilton *Data protection* 56–57.

214 DP Act of 1998 sch 1 part II par 3. The Directive (Dir 95/46/EC a 11(2) provides that member states must provide adequate safeguards when the exclusions are applicable. Presumably the Secretary of State will provide these safeguards in the "further conditions" he or she will prescribe.

215 Dir 95/46/EC recital 40.

consequences for the data subject.[216]

The Registrar (now the Commissioner) has advised that a number of factors should be taken into account, including (i) the cost to the data controller of providing the "fair processing information" weighed against the benefit to the data controller of processing the data; (ii) the length of time it would take the data controller to provide the information, again weighed against the benefit to the data controller; (iii) how easy or how difficult it would be for the data controller to provide the information, also weighed against the benefit to the data controller.

These factors should always be balanced against the effect on the data subject, that is the extent to which the withholding of the information may be prejudicial to the data subject. In this respect a relevant consideration would be the likelihood that or the extent to which the data subjects already know about the processing of their data by the data controller.[217]

3 Fairness in processing general identifiers

The Directive does not prohibit the use of a national identification number, but provides that member states should determine the conditions under which a national identification number or any other identifier of general application may be processed.[218] In response to this, the DP Act of 1998 provides that personal data which contain a general identifier,[219] defined by the Secretary of State by order, are not to be treated as having been processed fairly and lawfully unless they are processed in compliance with any conditions prescribed by the Secretary of State. [220]

---

216 Carey *Data Protection Act* 24.

217 See DPR *Data Protection Act 1998* 13.

218 Dir 95/46/EC a 8(7).

219 A "general identifier" means any identifier (such as a number or code used for identification purposes) which relates to an individual, and forms part of a set of similar identifiers which are of general application (DP Act of 1998 sch 1 part II par 4(1)).

220 DP Act of 1998 sch 1 part II par 4(2). Examples of general identifiers are National Health Service numbers (continued...)

ii Conditions for making data processing lawful

The first principle introduces a new requirement, not present in the DP Act of 1984, that as a pre-requisite for fair and lawful processing, no personal data may be processed unless at least one of the conditions in schedule 2 is present, and in the case of sensitive personal data, one of the conditions in schedule 3 as well. This new provision was necessitated by the provisions of the Directive, which prescribes that personal data may only be processed if one of six criteria is present, and which also prohibits the processing of sensitive data unless certain specific conditions are present.[221]

1 Conditions to be met before processing any personal data

At least one of the conditions of schedule 2 must be met in the case of all processing of personal data[222] (unless a relevant exemption applies).[223] In short, the data subject must have consented to the processing, or the processing must be **necessary** to comply with certain obligations, or to enhance certain legitimate interests, or to perform certain functions. In more detail, the conditions are:

❒ **The data subject has consented to the processing.**[224]

Consent is not defined in the DP Act. The Directive defines consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".[225] The Data Protection Registrar has advised that the fact that the data subjects are required to "signify" their agreement means that there must be some active communication

220(...continued)
and National Insurance numbers (Carey *Data Protection Act* 31).

221 Dir 95/46/EC aa 7 and 8.

222 DP Act of 1998 sch 1 part I par 1(a) and sch 2 (the conditions are spelled out in sch 2).

223 See par 4.3.6.

224 DP Act of 1998 sch 2 par 1.

225 Dir 95/46/EC a 2(h).

between the parties.[226] Data controllers cannot infer consent from non-response to a communication,[227] for example from a customer's failure to return or respond to a leaflet. Jay and Hamilton think that this interpretation may ring the death-knell for the "opt-out" approach to consent, which occurs where a data user notifies a data subject of a use to be made of personal data, and states that if a particular action is not taken, usually a box is not ticked, the consent of the subject will be assumed.[228] However, Lloyd argues that since "explicit" consent is required for processing sensitive data,[229] it must mean that the requirements for mere consent will be less stringent, and that the "opt-out" system would be compatible with this requirement.[230]

According to the Data Protection Registrar the adequacy of the purported consent must also be evaluated. A consent which was later found to have been obtained under duress or on the basis of misleading information would not be a valid basis for processing. The consent is not applicable for an indefinite period. Individuals may withdraw their consent. Consent must furthermore be appropriate to the particular circumstances. For example, if the processing to which it relates is intended to continue indefinitely or after the end of a trading relationship, then the consent should cover those circumstances.

226 DPR *Data Protection Act 1998* 10.

227 It is also a principle of common law that silence cannot indicate consent (*Attorney General v Jonathan Cape* [1975] 3 All ER 484).

228 Jay & Hamilton *Data protection* 40.

229 See subsequent par.

230 Lloyd *Data Protection Act 1998* 46. Note that under the 1984 Data Protection Act, the practice by British Gas Trading Ltd of informing their customers that data gathered for the purposes of customer administration would be used for the purpose of marketing products not associated with the supply of gas unless the customers positively signified their dissent was held to be unfair processing (see *British Gas Trading Ltd v Data Protection Registrar* (1998) (unreported) as quoted in Jay & Hamilton *Data protection* 79). Also see fn 199.

❒ **The processing is necessary for the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract.**[231]

The first leg of this condition means, for example, that if the data subject puts in a mail order, his or her personal data may be processed in order to obtain payment and effect delivery of the goods. The second leg of this condition appears to be designed to cover matters such as credit reference checks carried out by the data controller prior to entering into a contract with the data subject.[232] The term "necessary" is an important safeguard for the rights of data subjects, since it implies that the processing should not merely facilitate the performance of the contract, but that without it the performance will be impossible or impractical.[233]

❒ **The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.**[234]

This condition deals with the situation where a controller is obliged by law to process data. For example, if the law requires that schoolchildren be tested and that the test results be kept for a certain period, the school board does not have to seek the permission of the children's parents.[235] Similarly, since credit facilities may not be extended to persons under the age of eighteen years, a controller who

231 DP Act of 1998 sch 2 par 2.

232 Jay & Hamilton *Data protection* 79.

233 In Parliament it was explained that the word embodies the European legal principal of proportionality (Jay & Hamilton*Data protection* 80). The Constitutional principle of proportionality means that the infringement of privacy of the data subjects should not be out of proportion to the purpose that is served (see WBP *Memorie van toelichting* 8–9). Lloyd *Data Protection Act 1998* 46 points out that the word "necessary" appears in many instruments such as the European Convention on Human Rights and that the jurisprudence of the European Court of Human Rights has adopted an interpretation requiring that the practice in question be "close to essential" for the specified purpose.

234 DP Act of 1998 sch 2 par 3.

235 Jay & Hamilton *Data protection* 81.

is in the business of lending money may require that applicants provide information about their age.[236] Note that once more such processing must be "necessary".

❒ **The processing is necessary to protect the vital interests of the data subject.[237]**

The Commissioner considers that reliance on this exemption may only be claimed where the processing is necessary for matters of life and death, for example where a data subject's medical history is disclosed to a hospital casualty department treating the data subject after a serious road accident.[238] Although this is a restrictive interpretation open to question,[239] it is one that complies with the interpretation given by the Directive.[240] Once more the processing must be "necessary".

❒ **The processing is necessary for the administration of justice; for the exercise of any functions conferred on any person by or under any enactment; for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or for the exercise of any other functions of a public nature exercised in the public interest by any person.**[241]

There appears to be an overlap between this condition and the condition that permits processing where the processing is necessary for compliance with a legal obligation. The scope of this condition is broader, however, since it permits processing where the governing legislation simply empowers rather

236 Lloyd *Data Protection Act 1998* 46.

237 DP Act of 1998 sch 2 par 4.

238 DPR *Data Protection Act 1998* 8. Also see Carey *Data Protection Act* 27.

239 Jay & Hamilton *Data protection* 82.

240 "Vital interest" is described in the recitals par (31) of Dir 95/46/EC as "an interest which is essential for the data subject's life".

241 DP Act of 1998 sch 2 par 5.

than obliges a data controller to carry out a particular function.[242] Once more the processing must be "necessary".

❒ **The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.[243] The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.[244]**

According to Lloyd[245] and Jay and Hamilton,[246] this precondition is likely to prove one of the most, if not the most, contentious of the conditions for processing. Jay and Hamilton point out that the "legitimate interest" concept employed is an open-ended concept which is not further clarified and which has not been interpreted before.[247] This condition requires a balancing of interests – an assessment should be made of both the legitimate interests of the data subject and of those of the data controller and then an appraisal of which should take priority must be made.[248]

242 Jay & Hamilton *Data protection* 83.This condition will cover many public-sector data controllers.

243 DP Act of 1998 sch 2 par 6(1).

244 DP Act of 1998 sch 2 par 6(2). The DP Act of 1998 gives no further guidance on this condition, but Chalton et al *Encyclopedia of data protection* par 1–083/5 conclude that "legitimate interests" are broadly equivalent to "lawful activities", and that "prejudice to the rights and freedoms or legitimate interests of the data subject" bears a relationship to civil and human rights of individuals, including the right to respect for the individual's private and family life, his or her home and correspondence.

245 Lloyd *Data Protection Act 1998* 47.

246 Jay & Hamilton *Data protection* 85.

247 Jay & Hamilton *Data protection* 85. Bainbridge & Pearce 1998 *Computer L & Sec Rep* 259, 261 also think that "legitimate interests processing" will apply in a great many cases and will be relied upon by many data controllers. That being so, they regret that the concept is so vague. Also see Lloyd *Data Protection Act 1998* 47.

248 Jay & Hamilton *Data protection* 85. According to Bainbridge & Pearce 1998 *Computer L & Sec Rep* 259, 261 this condition is more restrictive than the corresponding one in the Directive. The Directive requires a balance between the legitimate interests of the controller and the rights and freedoms of the data subject.

(continued...)

These authors are further of the opinion that the "necessary" requirement that is again introduced can be given real teeth in this provision, because presumably many data controllers will attempt to process personal data on this condition where the pursuance of their legitimate interests is facilitated or helped by such processing, without such processing being essential or necessary to those interests.[249]

2 Additional conditions for processing sensitive personal data

In the DP Act of 1998 "sensitive personal data" means personal data consisting of information about the data subject's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, commission or alleged commission of any offence, being subject to proceedings for any offence committed or alleged to have been committed by the data subject, the outcome of such proceedings or the sentence of a court in such proceedings.[250]

The processing of such data may only take place if one of the conditions for the processing of data is met (schedule 2 conditions), as well as one of the following conditions (schedule 3 conditions):[251]

248(...continued)
The DP Act of 1998, on the other hand, requires that the rights and freedoms of the data subject should override the legitimate interests of the processor before processing is prohibited on this ground.

249 Jay & Hamilton *Data protection* 85. Jay and Hamilton also point out (at 86) that it should be remembered that although the data controller may be able to point to pursuit of his or her legitimate interests as a ground for processing personal data, this does do away with the requirement of the Act that the data subject should be informed about the purpose of the processing in order for the processing to meet the fair processing requirement of the first data protection principle. In other words, even if the condition for processing is present, processing may still be considered as not meeting the fairness requirement, and therefore be invalid.

250 DP Act of 1998 s 2. The first six grounds are similar to the special categories listed in the Directive, the processing of which are to be prohibited unless certain exceptions are applicable (see Dir 95/46/EC a 8(1)). The Directive does not specifically prohibit the processing of data relating to offences, criminal convictions or security measures, but provides that such processing may only be carried out under the control of an official authority or if suitable safeguards are provided under national law. Also see Bainbridge & Pearce 1998 *Computer L & Sec Rep* 180, 182.

251 DP Act of 1998 sch 1 part I par (1)(b) read with sch 3. See also DPR *Data Protection Act 1998* 9. The conditions listed in sch 3 mirror many of the conditions listed in sch 2. Compliance with a sch 3 condition may therefore sometimes also result in compliance with a sch 2 condition.

- **The data subject has given his or her explicit consent to the processing of the personal data.**[252]

There is a parallel requirement in schedule 2, but there is a difference between the consent required for the processing of all personal data, and the processing of sensitive personal data. In the last instance it is required that the consent should be "explicit". According to the Registrar, the use of the word "explicit" suggests that the consent of the data subject should be absolutely clear. In appropriate cases it should cover the specific detail of the processing, the particular type of data to be processed (or even the specific information), the purpose of the processing and any special aspects of the processing which may affect the individual, for example disclosures which may be made of the data.[253] Note that it is not required that the explicit consent should be in writing. However, it may be advisable for data controllers to get the consent in writing in order to avoid criticism as to whether the consent was clear and unambiguous.[254]

- **The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.**[255] The Secretary of State may by order specify particular circumstances in which this condition is either excluded altogether, or only satisfied upon the satisfaction of further conditions.[256]

This provision appears to be aimed at employers who wish to monitor the composition of their workforce in order to comply with the statutory duty on employers not to discriminate against

252 DP Act of 1998 sch 3 par 1.

253 DPR *Data Protection Act 1998* 11.

254 Jay & Hamilton *Data protection* 91.

255 DP Act of 1998 sch 3 par 2(1).

256 DP Act of 1998 sch 3par 2(2).

employees on the grounds of race,[257] sex[258] or disability.[259] In this respect this provision overlaps with another condition specifically providing for racial and ethnic data to be processed for this purpose.[260]

❒ **The processing is necessary to protect the vital interests of the data subject or another person, and consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject, or (in the case of the protection of the vital interests of another person) consent by or on behalf of the data subject has been unreasonably withheld.**[261]

The parallel requirement in schedule 2 is the condition that allows processing if it is necessary to protect the vital interests of the data subject. The meaning of "vital interest" will of course be the same for both provisions.[262] Jay and Hamilton point out that "curiously and atypically" the condition in schedule 3 appears to be more broadly framed than that in schedule 2, because it allows the processing of sensitive data when it is necessary to protect the vital interests of not only the data subject but also another person.[263] Another difference between the two conditions is the fact that the schedule 3 condition specifically refers to consent being given on behalf of the data subject, whereas the schedule 2 condition is silent on this issue.[264]

This condition deals with three scenarios in which the data subject's consent is not available:
(a) Consent cannot be given by or on behalf of the data subject (for example because the data subject

257 In terms of the Race Relations Act of 1976.

258 In terms of the Sex Discrimination Act of 1975.

259 In terms of the Disability Discrimination Act of 1996.

260 Jay & Hamilton *Data protection* 92.

261 DP Act of 1998 sch 3 par 3.

262 See text to fn 240.

263 Jay & Hamilton *Data protection* 93; Mullock & Leigh-Pollitt *Data Protection Act explained* 124.

264 For a discussion of the interesting lacuna that may be created by the inclusion of "consent on behalf of the data subject" in sch 3, and the omission thereof in sch 2, see Jay & Hamilton *Data protection* 95.

is in a coma). (b) The data controller cannot reasonably be expected to obtain the consent of the data subject (for example where a disclosure of the data subject's mental health is necessary to protect the vital interests of a third party, but seeking the consent of the data subject might seriously aggravate the situation). (c) Consent by or on behalf of the data subject has been unreasonably withheld (for example where a disclosure of a data subject's HIV positive status to his wife is necessary to protect her interests, but the data subject has unreasonably withheld his consent).[265]

- ❒ **The processing is carried out in the course of the legitimate activities of a body or association which was not established or is not conducted for profit, and exists for political, philosophical, religious or trade-union purposes.**

In this case the processing must be carried out with appropriate safeguards for the rights and freedoms of the data subjects,[266] should relate only to individuals who either are members of the body or association or have regular contact with it in connection with its functions, and does not involve disclosure of the personal data to a third party without the consent of the data subject.[267]

- ❒ **The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.**[268]

Difficulty may arise in interpreting "made public".[269] An obvious example would be where a person who is running for public office during an election expresses allegiance to a specific political party during a

265 Neither of the last two options, ie that processing of sensitive data is allowed where the controller cannot reasonably be expected to obtain the data subject's consent, or where the data subject unreasonably withholds consent, are in the Directive and the DP Act goes further than the Directive in these respects (see Bainbridge & Pearce 1998 *Computer L & Sec Rep* 259, 261).

266 Interpretive problems may arise with the concepts "rights and freedoms" and "appropriate safeguards" since the Act does not define these concepts.

267 DP Act of 1998 sch 3 par 4.

268 DP Act of 1998 sch 3 par 5.

269 The Directive requires that the data must have been "manifestly" made public (Dir 95/46/EC a 8(2)(e)).

radio broadcast. However, where a person makes the same statement at a dinner party for eight people, the information might not be considered to have been made "public".[270]

The information must have been made public "as a result of steps deliberately taken by the data subject". The fact that a person has a handicap may be publicly known, because it is obvious when looking at the person, but it is not certain whether this can be said to have been made public "as a result of steps deliberately taken by the data subject".[271]

This condition is one of the few that does not have a clear mirror provision in schedule 2, and a data controller must ensure that a schedule 2 condition is also satisfied when relying on this condition for processing sensitive data.[272]

❒ **The processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.**[273]

There is no qualification in this provision that ties the sensitive data to be processed to the person seeking the legal advice, or instituting the proceedings. For example, where a person seeks legal advice from an attorney, the data that are to be processed by the attorney need not be those of the person seeking the advice, but could be those of the opposing party.[274]

---

270 Also see Jay & Hamilton *Data protection* 97–98.

271 In terms of the Dutch Act (WBP), these data may not be processed in terms of this exemption, because the data have not been made known of the free will of the data subject (see Neth chap par 4.3.4.2). However, Jay & Hamilton *Data protection* 98 submit that the law cannot distinguish between a data subject that is visibly disabled and a data subject that has declared that he or she is disabled.

272 See Jay & Hamilton *Data protection* 98.

273 DP Act of 1998 sch 3 par 6.

274 Jay & Hamilton *Data protection* 98–99.

- **The processing is necessary for the administration of justice, for the exercise of any functions conferred on any person by or under an enactment, or for the exercise of any functions of the Crown, a Minister of the Crown or a government department.**[275] The Secretary of State may by order specify particular circumstances in which this condition is either excluded altogether, or only satisfied upon the satisfaction of further conditions.[276]

This condition mirrors a similar provision in schedule 2, apart from the fact that the Secretary of State may impose further conditions in the present one.

- **The processing is necessary for medical purposes and is undertaken by a health professional, or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.**[277]

"Medical purposes" include the purposes of preventive medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.[278] The term "health professional" is extensively defined in the Act.[279] There is no single clear parallel condition in schedule 2. As has been said, data controllers who intend processing sensitive data on a schedule 3 condition must also ensure that a schedule 2 condition is present. In cases where medical care is directly dispensed to the data subject, the consent condition of schedule 2 could be applicable. In cases of research or management, the public interest or legitimate interest conditions of schedule 2 may be

275 DP Act of 1998 sch 3 par 7(1). This condition for processing does not appear in the Directive. Member states are permitted to make additional conditions provided they incorporate suitable safeguards and are in the public interest (Dir 95/46/EC a 8(4)). No safeguards appear in the schedule. Also see Carey *Data Protection Act* 30.

276 DP Act of 1998 sch 3 par 7(2).

277 DP Act of 1998 sch 3 par 8(1).

278 DP Act of 1998 sch 3 par 8(2). The Directive's definition of medical purposes does not include medical research. According to Carey *Data Protection Act* 30 this has been a controversial addition to the Act by the UK government.

279 See DP Act of 1998 s 69.

appropriate.[280]

- **The processing involves sensitive personal data consisting of information as to racial or ethnic origin, but is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained.**

In this case the processing must be carried out with appropriate safeguards for the rights and freedoms of data subjects.[281] The Secretary of State may by order specify circumstances in which such processing is, or is not, to be taken as having been carried out with appropriate safeguards.[282]

We have already said that this condition overlaps with the condition that sensitive data may be processed where necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment. However, in this case the sensitive data to be processed may only relate to race or ethnic data.

- **The personal data are processed in circumstances specified in an order made by the Secretary of State.**[283]

The government has proposed that orders should be made to permit certain types of processing, namely to permit

280 See Jay & Hamilton *Data protection* 101.

281 DP Act of 1998 sch 3 par 9(1).

282 DP Act of 1998 sch 3 par 9(2).

283 DP Act of 1998 sch 3 par 10. The Directive permits member states to lay down exemptions in addition to the other specific exemptions provided for (Dir 95/46/EC a 8(4)). However, the Directive also provides that such exemptions must be for reasons of substantial public interest, that suitable safeguards must be provided, and that these exemptions must be laid down in national law or by the supervisory authority. The provisions of the DP Act of 1998 sch 3 par 10 do not contain these conditions. Also see Carey *Data Protection Act* 30.

– financial institutions and voluntary organisations (such as wildlife organisations) to process information about criminal offences and convictions for the purpose of detecting fraud and other offences;
– political parties to process information about political opinions in connection with canvassing;
– the police or other investigatory organisations to process various categories of sensitive data.[284]

4.3.4.3 *Second principle: obtaining and further processing of data for specified and lawful purpose*

The second principle requires that personal data may be obtained only for one or more specified and lawful purposes, and may not be further processed in any manner that is incompatible with such purpose or purposes.[285]

Under the DP Act of 1984 data were only to be treated as having been used for an incompatible purpose or disclosed in contravention of the principle if the use or disclosure was not registered with the Registrar. However, under the DP Act of 1998 compliance with this principle can no longer be established by merely registering the purposes for which data are processed. An additional test of compatibility will have to be satisfied to comply with this principle.[286]

In interpreting the second principle, the DP Act of 1998 provides[287] that the purpose or purposes for which personal data are obtained may in particular be specified in the notice given by the data controller

284 UK Home Office *Consultation paper on subordinate legislation* (1998) as quoted by Jay & Hamilton *Data protection* 102.

285 This principle gives effect to the requirement of the Directive that personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes (Dir 95/46/EC a 6(1)(b)).

286 DPR *Data Protection Act 1998* 14.

287 DP Act of 1998 sch 1 part II par 5.

to the data subject containing the "fair processing information" referred to above,[288] or in a notification to the Commissioner.[289]

Furthermore, in determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.[290]

The purpose for which data are collected should be lawful. The Act does not provide any guidance on the meaning of the word "lawful", but the Registrar has advised under the DP Act of 1984 that this means that a data user (data controller under the new Act) must comply with all relevant rules of law, whether derived from statute or common law, relating to the purpose for which the data user (controller) holds personal data and the ways in which the personal data are obtained and processed.[291] An example of an unlawful purpose would be if data were processed for the purpose of discriminating against someone.[292]

Jay and Hamilton question the necessity of the second principle, given that the first principle already requires the data controller to notify a data subject of the purposes for which data are intended to be processed. Processing without providing the specified information is then deemed unfair. Any processing for an incompatible (unspecified) purpose must consequently be unfair processing in breach of the first principle as well as in breach of the second principle.[293]

---

288 See text to fn 209.

289 On the notification procedure, see par 4.3.7

290 DP Act of 1998 sch 1 part II par 6.

291 DPR *Guidelines* 57.

292 Eg, an employment data base processed for purposes of discrimination against woman, which is in contravention of the Sex Discrimination Act of 1975. See Chalton et al *Encyclopedia of data protection* par 1–084.

293 Jay & Hamilton *Data protection* 61.

4.3.4.4 Third principle: adequate, relevant and not excessive data

The third principle requires that personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are being processed.[294]

No statutory interpretation is provided for this principle. However, the principle does not differ significantly from the equivalent principle in the DP Act of 1984, and guidelines by the Registrar under that Act can therefore be of use in interpreting the principle.

The Registrar has advised that this principle aims to ensure that the personal data held for a particular purpose are sufficient, but not more than sufficient for that purpose. Data users ("controllers" under the new Act) should seek to identify the minimum amount of information about each individual which is required in order to properly fulfil their purpose. If it is necessary to hold additional information about certain individuals, such information should only be collected and recorded in those cases.[295]

The relevance of data to a data user's purpose will be judged objectively. The adequacy, relevancy or excessiveness of data should be considered by each data controller in respect of each individual data subject. Holding data on the principle that they might be useful in future without knowing how the data could be useful is likely to be considered to be excessive.[296]

4.3.4.5 Fourth principle: accurate and up-to-date data

The fourth principle requires that personal data should be accurate and, where necessary, kept up to

294 This principle gives effect to a similarly worded provision in the Directive (Dir 95/46/EC a 6(1)(c)).

295 DPR *Guidelines* 61. Under the 1984 Act the Tribunal held in *Community Charge Registration Officer of Rhondda Borough Council v Data Protection Registrar* (1990) (unreported) that the holding of the dates of birth of every member of a household by a community charge registration officer was excessive. It was accepted, however, that holding dates of birth would be relevant in respect of those persons who would shortly become eligible to vote at the age of 18. See also Jay & Hamilton *Data protection* 62; Lloyd *Data Protection Act 1998* 52.

296 Chalton et al *Encyclopedia of data protection* par 1-087.

date.[297]

a Accuracy

The statutory interpretation of the fourth principle provides that the fourth principle is not to be regarded as having been contravened because of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party, as long as, having regard to the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data, and if the data subject has notified the data controller of the data subject's view that the data are inaccurate, the data indicate that fact.[298]

Data are inaccurate if they are incorrect or misleading as to any matter of fact.[299] Therefore, a mere opinion, which does not purport to be a statement of fact, cannot be challenged on the grounds of inaccuracy.[300]

The Registrar has advised under the DP Act of 1984[301] that the obligation of data users (data controllers under the 1998 Act) to ensure accuracy is not an absolute one, but that the issue is whether the data user has taken all reasonable steps to ensure accuracy.[302] Matters that will be considered are:

❒ the significance of the inaccuracy and whether it has caused or is likely to cause damage or

297 This principle is also intended to give effect to a similarly worded requirement in the Directive (Dir 95/46/EC a 6(1)(d)).

298 DP Act of 1998 sch 1 part II par 7.

299 DPR *Data Protection Act 1998* 14.

300 Jay & Hamilton *Data protection* 63.

301 DPR *Guidelines* 57.

302 This is also reflected in the requirements of the Directive, which requires that "reasonable steps must be taken" to erase or rectify inaccurate or incomplete data (Dir 95/46/EC a 6(1)(d)).

distress to the data subject

- whether the source of the information was reasonably relied on by the data user
- what steps were taken to verify the information, and whether the data user should reasonably have checked the information with the data subject
- procedures for data entry, and for avoiding the introduction of inaccuracies into the data
- procedures for discovering inaccuracies and for correcting inaccurate information already given, and other consequences

According to the Registrar, under the DP Act of 1998 it is no longer necessarily sufficient for data controllers to say that, because the information was obtained from either the data subject or a third party, they had done all that they reasonably could do to ensure the accuracy of the data themselves. Whether or not a data controller would be expected to take such steps will be a matter of fact in each individual case.[303] This principle obliges data controllers to accept information only from reliable sources and to take such steps as are practicable to verify the information prior to subjecting it to processing.[304]

b Kept up to date

The further requirement of the fourth principle that the data should be kept up to date "where necessary" is not expanded on in the statutory interpretation.

The Registrar has advised under the DP Act of 1984[305] that the necessity for updating is determined by the purpose for which the data are held – for example updating is unnecessary if the data are part of a historical record, but is necessary if they are used for a purpose such as credit rating. Other factors which the Registrar may take into account include:[306]

303 DPR *Data Protection Act 1998* 15.

304 Lloyd *Data Protection Act 1998* 60.

305 DPR *Guidelines* 64.

306 Updating of records may also be required by other statutes: eg certain spent records may not be referred (continued...)

- ❒ Is a record kept of the date when the information was recorded or last updated?
- ❒ Are all those involved with the data, including people to whom they are disclosed as well as employees of the data user, aware that they do not necessarily represent the current position?
- ❒ Does the data user take any steps to update the personal data, for example, by checking back at intervals with the original source or with the data subject? If so, how effective are these steps?
- ❒ Is the fact that the personal data are out of date likely to cause damage or distress to the data subjects?

4.3.4.6 Fifth principle: data not to be kept longer than is necessary for purposes for which they were collected

The fifth principle requires that personal data processed for any purpose or purposes may not be kept for longer than is necessary for such purpose or purposes.[307]

No statutory interpretation of this principle is provided. However, it corresponds to the sixth principle of the DP Act of 1984. The Registrar has advised under that Act that data users should review their personal data on a regular basis, setting a "life period" for specific records and establishing a review and delete procedure.[308]

In many cases controllers might be under an obligation to maintain data for a specified period of time. There would for example be a justification for keeping solicitor/client data until the expiry of any

306(...continued)
to after certain periods of time, and it is an offense under the Rehabilitation of Offenders Act of 1974 not to delete such a record from a data file (Chalton et al *Encyclopedia of data protection* par 1-090).

307 This principle implements a requirement of the Directive that personal data should not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected (Dir 95/46/EC a 6(1)(e)).

308 DPR *Guidelines* 64–65. By establishing such a procedure, the data user is also able to establish that data were destroyed under his or her authority, and thus evade a claim for compensation (see par 4.3.5.5).

limitation period for possible legal action.[309]

4.3.4.7 Sixth principle: processing in accordance with data subject's rights

The sixth principle requires that personal data must be processed in accordance with the rights of data subjects under the DP Act.

The statutory interpretation of this principle provides[310] that a person is to be regarded as contravening the sixth principle only if such a person:

- contravenes the right of access provisions of section 7 by failing to supply information in accordance with that section
- contravenes section 10 by failing to comply with a justified request to cease processing or by failing to respond to such a request within 21 days
- contravenes section 11 by failing to comply with a request to cease direct marketing processing
- in respect of exempt manual data (only during the transitional periods), fails to comply with a notice given under section 12 (the right to require the data controller to rectify, block, erase or destroy inaccurate data or cease holding such data in a manner incompatible with the data controller's legitimate purpose) or fails to give a notification under subsection (2)(a) of that section or a notice under subsection (3) of that section

These rights of the data subject will be dealt with further on.[311]

4.3.4.8 Seventh principle: appropriate level of security measures[312]

The seventh principle requires that appropriate technical and organisational measures be taken against

309 Lloyd *Data Protection Act 1998* 60.

310 DP Act of 1998 sch 1 part II par 8.

311 See par 4.3.5

312 For an extensive discussion of this principle, see Singleton *Data protection* 21–24.

unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.[313] The obligations imposed by this principle are reinforced by the obligation to notify the Commissioner of the security measures in place.[314]

The statutory interpretation of the seventh principle provides that,[315] having regard to the state of technological development and the cost of implementing any measures, the measures must ensure an appropriate level of security.[316] The appropriateness is determined with reference to the harm that might result[317] from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle and the nature of the data to be protected.

The data controller must take reasonable steps to ensure the reliability of his or her employees who have access to the personal data.[318] The Act imposes express obligations on data controllers when processing of personal data is carried out by a data processor on behalf of the data controller.

In order to comply with the seventh principle the data controller must:

313 This principle and its statutory interpretation give effect to the provisions of the Directive regarding the security of processing (Dir 95/46/EC a 17(1)–(4)). However, the Act falls short of the requirements of the Directive. Eg, the Directive's emphasis on the need for security "in particular where the processing involves the transmission of data over a network" has been left out, as well as the requirement that a processor may act only on instructions from the controller. Also see Jay & Hamilton *Data protection* 66.

314 DP Act of 1998 s 18(2)(b) (see also par 4.3.7).

315 DP Act of 1998 sch 1 part II par 9.

316 This implies that data controllers have to upgrade existing systems when technological advances occur. See Carey *Data Protection Act* 35; Pounder 1998 *Computers & Sec* 124, 125.

317 In this respect the Act differs from the Directive, which requires that the appropriateness must be determined with reference to the risks (not the harm) presented. However, in Parliament the government rejected an amendment that would have rephrased the interpretative provisions to make specific reference to the risks created, on the basis that it is the general principle of the law that a degree of damage or harm must be proved, and not simply the prospect of harm (see Lloyd *Data Protection Act 1998* 65). Lloyd argues that this approach is a case of closing the stable door after the horse has bolted.

318 DP Act of 1998 sch 1 part II par 10. Pounder 1998 *Computers & Sec* 124, 126 identifies three nuances to the word "reliable": staff can be made "reliable" by appropriate training in the correct security procedure; "reliable" staff are those individuals who have been vetted or approved, in advance of any access to personal data; staff become more reliable if the environment in which they work complies with best practice with respect to health and safety standards.

- choose a data processor that provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out[319]
- take reasonable steps to ensure compliance with those measures[320]
- ensure that the processing is carried out under a written contract which obliges the data processor to act only on instructions from the data controller and requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle[321]

4.3.4.9 Eighth principle: no transfer of data abroad unless an adequate level of protection is provided

a Introduction

The eighth principle requires that personal data may not be transferred[322] to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This principle, which is new to the UK data protection legislation, implements article 25 of the Directive which aims to harmonise the European Union's data protection provisions.[323] Within the EEA countries, there is no restriction on the transfer of data. Any transfer of data to a country outside the EEA is unlawful unless that country has an adequate level of protection.

---

319 DP Act of 1998 sch 1 part II par 11(a).

320 DP Act of 1998 sch 1 part II par 11(b).

321 DP Act of 1998 sch 1 part II par 12. According to Pounder 1998 *Computers & Sec* 124, 126 this requirement implies that the data controller has to be fully aware of the broad nature of the security procedures adopted by a chosen data processor.

322 The Act does not give a definition for "transfer", but presumably it should be given its ordinary meaning, ie transmission from one place, person etc to another (see Jay & Hamilton *Data protection* 109). Bainbridge *Data protection law* 97–99 discusses the importance of establishing whether a "disclosure" of information, where no transfer takes place, will be deemed to be included under the term "transfer".

323 Dir 95/46/EC a 25. See ch 3 par 4.2.7.

b Determining adequacy

The DP Act contains an interpretation of this principle.[324] According to this, an adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to the following:[325]

- **The nature of the personal data**

The Registrar points out that there is a difference between the transfer of sensitive data and the transfer of personal data that are widely available, for example information about well-known public figures (such as the transfer of personal data on professional football players between football clubs around the world.[326]

- **The country or territory of origin of the information contained in the data**

This is not the country from which the transfer originates but rather the country from which the data originate. In most cases this is where the information was originally obtained. Where the information has been obtained in a third country this will be a relevant factor to consider because the data subjects may have different expectations as to the level of protection that will be afforded to their data than they would have had if the information been obtained within the EEA.[327]

- **The country or territory of final destination of that information**

In some cases it may be known that there will be a further transfer to another country which may or may

---

324 DP Act of 1998 sch 1 part II para 13–15.

325 These circumstances are also found in the Directive (see Dir 95/46/EC a 25(2)).

326 DPR *The eighth data protection principle and TBDF* 10.

327 DPR *The eighth data protection principle and TBDF* 10.

not be outside the EEA. If data originate in a third country, are transferred for processing in an EEA state and then returned to the original third country, the level of protection afforded to those data may not be required to be greater than the protection a citizen of the country of origin would have expected.[328]

- **The purposes for which and period during which the data are intended to be processed**

The longer the period of processing the more likely it is that any deficiencies in the legal protection will be exposed. Any data controller who proposes to set up a permanent operation in a third country and anticipates making regular large-scale transfers to that country should make a detailed analysis of the adequacy standard.[329]

The next four criteria require the data controller to consider the data protection regime in place in the country of destination, specifically:

- **The law in force in the country or territory in question**

- **The international obligations of that country or territory**

- **Any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases)**

- **Any security measures taken in respect of the data in that country or territory**

The Registrar is of the opinion that in practice it may often be the case that security will be the key factor in ensuring adequacy. Exporting controllers may ensure that personal data are secure from outside interference by means of technical measures such as encryption or the adoption of information

328 DPR *The eighth data protection principle and TBDF* 10.

329 DPR *The eighth data protection principle and TBDF* 11.

security management practices.[330]

This is not an exhaustive list of criteria for consideration.[331] According to Carey,[332] the most relevant factor of all is missing, namely the existence of a contract between the transferor and the transferee. The Directive refers to "appropriate contractual solutions" as an additional factor for consideration.[333] However, the Registrar has advised that the English law doctrine of privity of contract[334] presents problems regarding the use of contracts to secure rights for third parties.[335] Exporting controllers will therefore have to satisfy themselves that a proposed contract purporting to secure adequacy effectively overcomes the problems of privity (for example by adopting the law of another jurisdiction which recognises third party rights).[336]

The Directive envisages that the European Commission could make a finding in respect of a non-member country on the adequacy of that country's data protection rules.[337] The DP Act of 1998 provides[338] that where such a finding has been made, any question on the adequacy of protection provided in a third country (that is, a country outside the EEA)[339] must be determined in accordance

330 DPR *The eighth data protection principle and TBDF* 10.

331 DPR *The eighth data protection principle and TBDF* 5.

332 Carey *Data Protection Act 1998* 36.

333 Dir 95/46/EC a 26.

334 This doctrine provides that, as a general rule, a contract cannot confer rights or impose obligations arising under it on any person except the parties to it (Jay & Hamilton *Data protection* 119).

335 In Scottish law third party rights can be created where the doctrine of *jus quaesitum tertio* applies. See DPR *The eighth data protection principle and TBDF* 14.

336 See DPR *The eighth data protection principle and TBDF* 14–15.

337 See Dir 95/46/EC a 30(1)(b). The procedure for doing this is prescribed in a 31.

338 DP Act of 1998 sch 1 part II par 15.

339 See fn 160 on the members of the EEA.

with that finding.[340]

c Exemptions from eighth principle

The DP Act, following the Directive,[341] also provides for derogations, or circumstances where the eighth principle does not apply to a transfer of data (except in such circumstances and to such extent as the Secretary of State may by order provide).[342] Broadly speaking, the exemptions cover two situations, first where the risks to the data subject are relatively small and second, where other interests (public interests or those of the data subject himself or herself) override the data subject's right to privacy.[343]

Even if the country in question does not meet the adequacy standard, a transfer of data may still take place if:[344]

- the data subject has consented to the transfer
- the transfer is necessary for the performance of a contract between the data subject and the data controller, or for the taking of steps at the request of the data subject with a view to entering into a contract with the data controller[345]

340 DPR *Data Protection Act 1998* 15. During 2002 the EU has ruled that Switzerland and Hungary provide adequate protection (EPIC *Privacy and human rights* 15).

341 See Dir 95/46/EC a 26(1).

342 DP Act of 1998 sch 1 part II par 14 read with sch 4.

343 Jay & Hamilton *Data protection* 121.

344 Note that there are many similarities between the exemptions and the conditions for processing, and comments made in that regard (see par 4.3.4.2) are also relevant here.

345 The "contractual transfers" are broader than in the Directive which does not cover taking steps with a view to entering into a contract with the data subject (see Bainbridge & Pearce 1998 *Computer L & Sec Rep* 259, 264).

- ❒ the transfer is necessary for the conclusion of a contract between the data controller and a person other than the data subject (entered into at the request of the data subject, or entered into in the interests of the data subject) or for the performance of such a contract

- ❒ the transfer is necessary for reasons of substantial public interest

  (The Secretary of State may by order specify circumstances in which a transfer is to be taken, or not to be taken, as necessary for reasons of substantial public interest.)

- ❒ the transfer is necessary for any legal proceedings or for obtaining legal advice, or for the purposes of establishing, exercising or defending legal rights

- ❒ the transfer is necessary in order to protect the vital interests of the data subject

- ❒ the transfer is part of the personal data on a public register and the conditions subject to which the register is open to inspection have been complied with by the person to whom the data are or may be disclosed after the transfer

- ❒ the transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects

- ❒ the transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects[346]

The Registrar has advised[347] that in assessing adequacy, data controllers should follow a "good practice approach" consisting of four steps: (i) Consider whether (or the extent to which) the third country in question is to be the subject of a community finding or presumption of adequacy. (ii) Consider the type

346 The last two exceptions are allowed by Dir 95/46/EC a 26(2).

347 DPR *The eighth data protection principle and TBDF* 5.

of transfer involved and whether this enables any presumption of adequacy (for example, in the case of controller to processor transfers), or of inadequacy (for example transfers which amount to a sale of data to a third party with no continuing relationship either with the data subject or the purchaser). (iii) Consider and apply the "adequacy test", including consideration of the application and use of contracts and/or codes of conduct to create adequacy. (iv) Where there is no adequacy, or where there is doubt in this respect, look to the derogations contained in schedule 4 of the Act, pursuant to which transfer may proceed if any of them are satisfied.

4.3.5 Rights of data subjects

Part II of the DP Act of 1998 spells out the rights of data subjects. These rights are a right of access to his or her personal data (section 7); a right to prevent processing that is likely to cause damage or distress (section 10); a right to prevent processing for purposes of direct marketing (section 11); a right to object to automated decision-taking (section 12); a right to compensation for failure by a data controller to comply with the requirements of the Act (section 13); a right to approach the court to order the data controller to rectify, block, erase or destroy data (section 14); and lastly a right to request the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened (section 42). In some cases these rights extend not only to data subjects but to "individuals" or "persons".[348] The DP Act of 1998 also provides for exemptions from part II of the Act. These exemptions will be discussed later on.[349]

As will be seen, four of these rights, namely the right to have subject access, the right to object to processing, the right to object to direct marketing and the right to object to automated decision-making, are exercised by a notice or request in writing to the data controller. No formalities are prescribed as to how the notices or requests should be served. Service by electronic means is allowed as long as the

348 See eg the right to prevent processing likely to cause damage or distress (par 4.3.5.2), the right to prevent processing for direct marketing purposes (par 4.3.5.3), the right to compensation (par 4.3.5.5) and the right to request an assessment (par 4.3.5.7).

349 See par 4.3.6.

notice is received in legible form and is capable of being used for subsequent reference.[350] As to the exercise of rights by minors, the Act provides that a child of twelve years or over will be presumed to have sufficient age and maturity to exercise any rights conferred by the Act.[351] Parents or guardians will have to act on behalf of children under the age of twelve. A data subject may also appoint someone else to exercise his or her rights under the Act.[352]

4.3.5.1 Right of access to personal data

Commentators point out that in the framework of individual rights in relation to personal information established by the DP Act of 1998, subject access may be regarded as the threshold provision for the exercise of those rights. Unless individuals can learn what information is held about them and what will happen to it, their rights to correct or challenge it may become valueless.[353]

As required by the Directive,[354] the DP Act of 1998 provides data subjects with a right to access their personal data.[355] This right can also be described as a right to be informed about certain aspects

350 DP Act of 1998 s 64.

351 DP Act of 1998 s 66.

352 See also Jay & Hamilton *Data protection* 156. These authors also discuss the question whether a party may contract out of the individual rights. In the end they conclude that it may be lawful for a private body to seek to exclude the individual right to go to court to enforce the remedies granted for breach of the individual rights in ss 7, 10, 11, 12, 13 and 14, subject to the requirement that the contract be fair and not in breach of the Unfair Terms in Consumer Contracts Regulations of 1994. If one party does not honour the agreement it may not be enforceable in the court after implementation of the Human Rights Act. In their opinion, it would not be lawful for a public body to seek to exclude those rights, and it will not be lawful for anybody to seek to exclude the powers of the Commissioner or the right to complain to the Commissioner. See also Jay & Hamilton *Data protection* 159.

353 Jay & Hamilton *Data protection* 162.

354 Dir 95/46/EC a 12(a).

355 The Directive also requires member states to provide data subjects with the right to obtain from the controller the rectification, erasure or destruction of data which do not comply with the provisions of the Directive, in particular because they are incomplete or inaccurate (Dir 95/46/EC a 12(b)). Third parties to whom data have been disclosed should also be notified about any rectification, erasure or blocking carried out on the data involved (Dir 95/46/EC a 12(b)). The DP Act of 1998 does not contain provisions fulfilling these last two requirements. As we will see, data subjects do have the right to approach the court to order

(continued...)

surrounding the processing of the subject's personal data. The DP Act also prescribes procedures for dealing with access requests, especially when information about other people is also involved. Further, it contains a special reference to access requests directed to credit reference agencies.

a Content of right

The DP Act of 1998 provides firstly that an individual is entitled to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.[356] If that is the case, the data subject is entitled to be given a description by the data controller of the personal data of which that individual is the data subject, the purposes for which they are being or are to be processed, and the recipients or classes of recipients to whom they are or may be disclosed.[357]

The individual is also entitled to have communicated to him or her in an intelligible form the information constituting the personal data of which that individual is the data subject.[358] This should be a copy of the information in permanent form, unless it is impossible to provide or would involve a disproportionate effort, or unless the data subject agrees otherwise. Where any of the information is expressed in terms which are not intelligible without explanation, the copy must be accompanied by an explanation of those

355(...continued)
the data controller to erase, block or destroy data, but the Act does not provide them with a right to directly request the controller to do so.

356 DP Act of 1998 s 7(1)(a). S 7 states that the data subject is "entitled" to the information concerned but does not go so far as to require the controller to give all the information if it is not specifically asked for by the data subject. Presumably the Secretary of State will prescribe in regulation that a controller should treat a request for any information as extending to other information to be given under s 7. See Bainbridge & Pearce 1998 *Computer L & Sec Rep* 401. Under the new Act it is also possible for a data subject to specify that his or her request for access is limited to personal data of a prescribed form (DP Act of 1998 s 7(7)). This was not possible under the DP Act of 1984 (see *R v Chief Constable of B County Constabulary; Director of National Identification Services, ex p R* Nov 1997 (unreported) (as quoted in Jay & Hamilton *Data protection* 165).

357 DP Act of 1998 s 7(1)(b). "Recipient" is defined in the DP Act of 1998 s 70 (see par 4.3.3.1). According to this definition, a person to whom disclosure is made as a result of a particular inquiry by that person made in the exercise of any power conferred by law is not a recipient. This means that a data controller does not have to tell the data subject that the information will be disclosed to, eg, the Inland Revenue Service.

358 DP Act of 1998 s 7(1)(c)(i). As previously stated, the DP Act of 1998 draws a distinction between "data" and "information": data are information that is recorded or processed in a certain way (see par 4.3.3.1).

terms.[359]

The individual is also entitled to have communicated to him or her any information available to the data controller as to the source of those data.[360] However, in some instances the data controller is not obliged to disclose such information where the source of the data is, or can be identified as, an individual.[361]

Where a decision significantly affecting data subjects is, or is likely to be, made about them by fully automated means, for the purpose of evaluating matters about them such as their performance at work, their creditworthiness, their reliability or their conduct, they are entitled to be told of the logic involved in that process.[362] The data controller is not required to do this where the information in question constitutes a trade secret.[363]

b Procedures for dealing with subject access requests

Data controllers are not obliged to supply any information unless the requests to access were in writing,

359 DP Act of 1998 s 8(2). Eg, where the data controller holds the information in coded form which cannot be understood without the key to the code (see DPR *Data Protection Act 1998* 17).

360 DP Act of 1998 s 7(1)(c)(ii). This is a new right in the DP Act of 1998 (see Carey*Data Protection Act 1998* 10). Data controllers are not obliged by the Act to retain information about data sources and it will be up to the data controller to decide how much information to keep. The sources of data no longer have to be notified on the public register, as was the case under the 1984 Act. See also Jay & Hamilton *Data protection* 168.

361 DP Act of 1998 s 7(4) read with s 7(5) (see DPR *Data Protection Act 1998* 17).

362 DP Act of 1998 s 7(1)(d).

363 DP Act of 1998 s 8(5). The Act does not define "trade secret"– see DPR *Data Protection Act 1998* 17. Bainbridge & Pearce 1998 *Computer L & Sec Rep* 401, 402 argue that it would be sensible to give trade secret the same meaning as in the law of breach of confidence. One approach would then be to consider a trade secret in this context as information the disclosure of which could harm the controller's legitimate interests or be of benefit to a competitor. The Law Commission in a consultation paper on trade secrets published in 1997 (referred to in Jay & Hamilton *Data protection* 168–169) gave the following definition: "information which is not generally known, which derives its value from that fact and as to which its owner has indicated (expressly or implied) his or her wish to preserve its quality of secrecy".

and a required fee was paid.[364] The data controllers may also require information in order to satisfy themselves as to the identity of the persons making the requests before complying with such requests.[365] Data controllers must respond promptly to a request for access, and in any event before forty days have passed since receiving the request, the fee and all the relevant information required in order to comply with the request.[366] Data controllers do not need to comply with a request where they have already complied with an identical or similar request by the same individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.[367] In deciding what amounts to a reasonable interval, the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered should be considered.[368]

The information to be supplied pursuant to a subject access request must be supplied by reference to the data in question at the time when the request was received. Account may be taken of any routine amendments or deletions made between that time and the time when the information is supplied.[369] The important thing is that having received a request, the data controller must not make any special amendment or deletion which would not otherwise have been made. The information must not be tampered with in order to make it acceptable to the data subject.[370]

c Third party information[371]

364 The fee may not exceed a certain maximum, and in certain prescribed cases no fee may be asked (DP Act of 1998 s 7(2)). At the time of writing the maximum fee had not yet been determined, but under the DP Act of 1984 it was £ 10 (see Singleton *Data protection* 29).

365 DP Act of 1998 s 7(3).

366 DP Act of 1998 ss 7(8) and 7(10).

367 DP Act of 1998 s 8(3).

368 DP Act of 1998 s 8(4).

369 DP Act of 1998 s 8(6).

370 DPR *Data Protection Act 1998* 18.

371 For a detailed discussion of the issue of third party data, see Jay & Hamilton *Data protection* 170–174. They indicate that these provisions should be seen as an incorporation into UK law of the decision of the (continued...)

Where a data controller cannot comply with the request without disclosing information relating to another individual who could be identified from that information, including being identified as the source of the information,[372] the controller is not obliged to comply with the request unless:

- the other individual has consented to the disclosure of the information to the person making the request
- it would be reasonable in all the circumstances to comply with the request without the consent of the other individual[373]

However, the data controller is not excused from communicating as much of the requested information as can be communicated without disclosing the identity of the other individual concerned, for example by the omission of names or other identifying particulars.[374]

In determining whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard must be had, in particular, to–

- any duty of confidentiality owed to the other individual
- any steps taken by the data controller with a view to seeking the consent of the other individual
- whether the other individual is capable of giving consent
- any express refusal of consent by the other individual

If a data controller is satisfied that the data subject will not be able to identify the other individual from the information, taking into account any other information which, in the reasonable belief of the data controller, is likely to be in (or to come into) the possession of the data subject, then the data controller

371(...continued)
Court of Human Rights in *Gaskin v United Kingdom* [1989] 12 ECHR 36 (on the *Gaskin* case, see fn 134).

372 Eg, where a social worker or person in charge of a home for children in care has written a report on the person now making the subject access request, the consent of the social worker must be obtained, or it must be reasonable to comply without the consent (Bainbridge *Data protection law* 118).

373 DP Act of 1998 s 7(4).

374 DP Act of 1998 s 7(5).

must provide the information.[375]

d Credit reference agencies

There are slight modifications to the right of access where the data controller is a credit reference agency.[376] Where this is the case, a subject access request received under the DP Act of 1998 may be limited to personal data relevant to the individual's financial standing and, unless the request shows a contrary intention, will be deemed to be so limited.[377] The data controller is also obliged to give the individual making the request a statement, in such form as may be prescribed by the Secretary of State in regulations, of the individual's rights under section 159 of the Consumer Credit Act of 1974, and to the extent required by the prescribed form, under the DP Act.[378]

e Remedies

If a data subject believes that a data controller has failed to comply with a subject access request in contravention of the Act he or she may apply to court for an order compelling the data controller to comply with the request. An order will be made if the court is satisfied that the data controller has failed to comply with the request in contravention of the Act.[379] The data subject will also have the right to

375 DP Act of 1998 s 8(7). Also see DPR *Data Protection Act 1998* 18.

376 DP Act of 1998 s 9(1) and see Carey *Data Protection Act 1998* 13.

377 DP Act of 1998 s 9(2).The law of breach of confidence has long since regulated the disclosure of personal data by financial institutions (see *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461). See also Bainbridge *Data protection law* 122.

378 DP Act of 1998 s 9(3). The DP Act of 1998 incorporates the rights of access previously granted to data subjects under the Consumer Credit Act of 1974, the Access to Personal Files Act of 1987, the Access to Health Records Act of 1990 and the Education (School Records) Regulations of 1989 (schedule 16) (see Chalton et al *Encyclopedia of data protection* par 1–232). These Acts are either repealed or amended by the DP Act of 1998 (see schs 15 and 16).

379 DP Act of 1998 s 7(9). For the purpose of determining whether an applicant under this subsection is entitled to the information which he or she seeks, a court may require the information constituting any data processed by or on behalf of the data controller and any information as to the logic involved in any automated decision-taking to be made available for its own inspection but may not, pending the determination of that question in the applicant's favour, require the information sought by the applicant

(continued...)

seek compensation.[380] The Commissioner may also serve an enforcement notice on the controller requiring him or her to provide subject access.[381]

f Prohibition on enforced subject access

Data subjects may not be forced to supply records obtained by them under their right to access where these records relate to health data, cautions, criminal convictions and certain social security records relating to the data subject.

First of all, any term or condition of a contract is void in so far as it purports to require an individual to supply any other person with a record obtained under the data subject's right to access, where this record consists of the information contained in any health record, or with a copy of such a record or a part of such a record, or to produce to any other person such a record, copy or part.[382]

Secondly, is it an offence to require that a person supply a record relating to cautions, criminal convictions and certain social security records in connection with recruitment, continued employment or contracts for the provision of services.[383] This provision does not derive from the Directive or from earlier legislation, but was inserted in response to a problem that has developed in the UK since the passing of the 1984 Act. Often prospective employers made it a condition of offering employment to individuals that they make a subject access request to the police and provide the result to the employers. In this manner the employers could check whether the individuals have criminal records.[384]

379(...continued)
to be disclosed to him or her or his or her representatives (DP Act of 1998 s 15(2)).

380 See par 4.3.5.5.

381 See par 4.3.8.3.

382 DP Act of 1998 s 57(1). A health record means a record which consists of information relating to the physical or mental health or condition of an individual which has been made by or on behalf of a health professional in connection with the care of that individual (DP Act of 1998 s 68(2)).

383 DP Act of 1998 s 56. See also par 4.3.10.2.

384 See also Jay & Hamilton *Data protection* 328–338. *R v Chief Constable of 'B' ex parte R* (1997) (unreported) 1997 provides an example of the practice. The case is discussed by Bainbridge *Data* (continued...)

4.3.5.2 Right to prevent processing likely to cause damage or distress

a Content of right

An individual is entitled to serve upon a data controller a written notice (called a "data subject notice")[385] requiring the data controller not to process personal data of which that individual is the data subject, where such processing is likely to cause unwarranted substantial damage or distress to the individual or to another individual.[386] The individual must show both that the processing will cause substantial damage or distress and that the damage or distress will be unwarranted. Jay and Hamilton point out that "substantial" is one of those concepts, like "significant" or "reasonable", that import the concept of proportionality and thus greatly depend on context.[387] They suggest that the test for determining whether distress is substantial, should be objective, otherwise an individual's right will vary, depending on his or her sensibilities.[388] Determining whether the distress or damage is "unwarranted" entails a balancing test between the reasons for processing and the effect on the individual. The two most obvious reasons why processing could be unwarranted are that the processing would amount to a breach of the individual's private or family life, or that the processing would amount to a breach of the data protection principles.[389]

The object of this provision is to give effect to the requirement of the Directive that member states must grant data subjects the right to object to processing where processing is for direct marketing

384(...continued)
protection law 122.

385 See DPR *Data Protection Act 1998* 18.

386 DP Act of 1998 s 10(1). This is a qualified right, in the sense that a balancing test must be applied, whereas the right to object to processing for direct marketing granted in s 11 (see par 4.3.5.3) is an absolute right (see Chalton et al *Encyclopedia of data protection* par 1–060/5; Jay & Hamilton *Data protection* 191).

387 Jay & Hamilton *Data protection* 196.

388 Jay & Hamilton *Data protection* 197.

389 Jay & Hamilton *Data protection* 197.

purposes[390] or where processing takes place because it is necessary for:[391]

- ❒ the performance of a task in the public interest or in the exercise of an official authority
- ❒ the purposes of the legitimate interests of the controller or third parties[392]

b Exclusions

This right is unavailable where any one of the first four conditions for processing is complied with, in other words where the data subject has consented to the processing; where the processing is necessary to perform a contract or for the data subject to enter into a contract; where the data controller has to process the data to comply with a legal obligation; or where the processing is necessary to protect the vital interests of the data subject.[393] This right is also unavailable in such other cases as may be prescribed by order of the Secretary of State.[394]

c Procedure

The data controller has twenty-one days to respond in writing to the data subject's notice. The data controller must indicate whether he or she intends to comply with the data subject's notice and the extent to which he or she intends to comply, or state his or her reasons for regarding the notice as

390 See Dir 95/46/EC a 14(b).

391 Dir 95/46/EC a 14(a)).

392 The DP Act of 1998 gives effect to the requirement of the Directive in a roundabout way: It provides that data subjects have a right to object to processing on the grounds that it is likely to cause damage or distress, but not where the processing is taking place pursuant to the first four conditions, thus leaving only the last two conditions, which are similar to the two conditions found in the last situation provided for by the Directive.

393 DP Act of 1998 sch 2. There are two other conditions for processing, the first one dealing with processing that is necessary for a task that is in the public interest, eg administration of justice, and the other dealing with processing that is necessary for the purposes of the legitimate interests of the data controller or third parties (see par 4.3.4.2 above).

394 DP Act of 1998 s 10(2). No order was immediately proposed (see DPR *Data Protection Act 1998* 18). Jay & Hamilton *Data protection* 199 indicate that this right will be most useful where the individual is dealing with specific data or specific relationships which are not contractual, eg data recorded and processed during pre-contractual negotiations.

unjustified.[395]

d Remedies

Where the data subject considers that the data controller has not complied with a a notice he or she can seek a court order. If the court agrees it can order the data controller to take such steps as are necessary to comply with the notice.[396] The Commissioner may also serve an enforcement notice on the controller.[397] The failure by a data subject to exercise the right to object to processing does not affect any other right conferred on him or her by part II of the Act.[398]

4.3.5.3 Right to prevent processing for direct marketing purposes

a Content of right

The Directive grants data subjects a right to object to processing for the purposes of direct marketing, "or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing".[399] The DP Act of 1998 implements the first part of this provision[400] by providing that an individual is entitled at any time, by written notice, to require a data controller at the end of a reasonable period to cease, or not to begin, processing personal data relating

395 DP Act of 1998 s 10(3).

396 DP Act of 1998 s 10(4). Bainbridge & Pearce 1998 *Computer L & Sec Rep* 401, 403 find it difficult to think of a situation where such a notice would be justified if the processing is otherwise in compliance with the data protection principles.

397 See par 4.3.8.3.

398 DP Act of 1998 s 10(5).

399 Dir 95/46/EC a 14(b).

400 However, Chalton et al *Encyclopedia of data protection* par 1–246/2 point out that the further element of the Directive (in quotations) is not present in the DP Act of 1998, which would appear to be a significant limitation of the rights being granted to the data subject.

to that individual for the purposes of direct marketing.[401] "Direct marketing" is defined in the Act for the purposes of this provision as the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.[402] These provisions cover processing directly aimed at producing personal mail, faxes, telephone calls or any other form of communication. They also cover host mailings, that is, inserts with other mail. These provisions may also enable an individual to require a controller to desist from profiling, screening or data-mining activities even where they do not result in the direct arrival of marketing materials to the individual.[403] The use of "cookies"[404] for marketing and selling purposes will amount to direct marketing within the meaning of the Act.[405]

b Remedies

If the data controller fails to comply with the notice, the data subject may apply to court for an order to that effect. If the court is satisfied that the data controller has failed to comply with the notice, the court may order the data controller to take such steps for complying with the notice as the court thinks fit.[406] Failure to comply with an individual's objection may also lead to enforcement by the Commissioner.[407]

---

401 DP Act of 1998 s 11(1). This is an absolute right (Chalton et al *Encyclopedia of data protection* par 1–060/5; Bainbridge & Pearce 1998 *Computer L & Sec Rep* 401, 403) and it is equivalent to a strict liability provision (Jay & Hamilton *Data protection* 192).

402 DP Act of 1998 s 11(3). The UK government also implemented the direct marketing component of the European Commission's Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Dir 97/66/EC) – also called the ISDN Directive because it partially relates to the Integrated Services Digital Network (see Singleton*Data protection* 79). In December 1998, the UK adopted the Telecommunications (Data protection and Privacy) (Direct Marketing) Regulations. These regulations impose strict controls on the use of automated calling systems, facsimile machines and simple voice telephones for making unsolicited contact with a subscriber for direct marketing purposes (see Chalton et al *Encyclopedia of data protection* par 1–246/3).

403 See Jay & Hamilton *Data protection* 192.

404 For a definition of "cookies", see ch 1 par 1.3.

405 Carey *Data Protection in the UK* 146 et seq.

406 DP Act of 1998 s 11(2).

407 See par 4.3.8.3.

4.3.5.4 Rights in relation to automated decision taking

The Directive prescribes that an individual must have the right not to be subject to evaluative decisions concerning him or her where such decisions are based solely on the automated processing of personal data. Exceptions may be made where the decision is taken in the context of a contract or where it is authorised by law, provided the data subject's legitimate interests are safeguarded.[408]

a Content of right

In this regard, the DP Act of 1998 provides that an individual is entitled at any time, by written notice to any data controller, to require the data controller to ensure that no decision which significantly affects him or her is based solely on the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to such individual.[409] The Act gives examples of the purposes for which such automated decision taking might be employed, namely the evaluation of matters relating to the data subject such as performance at work, creditworthiness and his or her reliability or conduct. This is not an exhaustive list.[410] It should also be emphasised that the right of objection only applies where processing is carried out to make assessments or pass judgment on individuals. Also, the assessment or evaluation must be capable of resulting in a decision which "significantly affects" the individual.[411] Furthermore, the prohibition can be applied only where the

408 Dir 95/46/EC a 15. This provision was included on the insistence of the French, and it "represents a totally novel departure for UK law" (see Slee 1999 *Inf & Comm Tech L* 71, 91).

409 DP Act of 1998 s 12(1). The provisions of the DP Act clearly fall short of those of the Directive, which allow automated decision taking only in restricted circumstances. The Act, on the other hand, does not prohibit such processing but merely gives the data subject the right to prevent it by means of a written notice (Bainbridge & Pearce 1998 *Computer L & Sec Rep* 259, 262). Also note that this is not an absolute right, and if the individual's objection is ignored the furthest the individual can go is to ask the court to order the data controller to reconsider the original decision (see Chalton et al *Encyclopedia of data protection* par 1–060/6).

410 See DPR *Data Protection Act 1998* 19.

411 "Significantly effects" is not defined. Presumably the decision does not necessarily have to result in physical damage or financial loss, but may also cause emotional distress. Note that the section does not require that the effect on the individual should be detrimental, but it is unlikely that an individual will object to receiving an unsolicited benefit (Jay & Hamilton *Data protection* 210).

decision is based solely on automated processing. Human intervention, however slight, will negate this prohibition.[412]

Where the individual has not given notice to the data controller to prevent automated decision-taking,[413] a data controller who takes an automated decision is nevertheless obliged to notify[414] the individual "as soon as is reasonably practicable" that such a decision was taken (except if it as an exempt decision).[415] The individual may then request the data controller in writing to reconsider the decision or to take a new decision on another basis.[416] The controller must respond in writing, specifying the steps that he or she intends to take to comply with the data subject's notice.[417]

b Remedies

A data subject may apply for a court order requiring a person taking a decision in respect of the data subject (referred to in the Act as "the responsible person") to reconsider the decision or to take a new decision which is not based solely on processing by automatic means. The court will only make such an order if it is satisfied that the responsible person has failed to comply with notices from the data subject.[418] The court order does not affect the rights of any person other than the data subject and the responsible person.[419]

---

412 Jay & Hamilton *Data protection* 210.

413 Or where the notice has not been given in a proper manner, also resulting in the absence of a notification (see Carey *Data Protection Act 1998* 16).

414 The DP Act of 1998 does not specify whether this should be in writing or not.

415 Exempt decisions are discussed later on. (See par c below.)

416 DP Act of 1998 s 12(2). Jay & Hamilton*Data protection* 214 suggest that the data controller should refrain from implementing a decision taken by automatic means until the individual has had time to object to such decision, if he or she should choose to do so.

417 DP Act of 1998 s 12(3). In each case the data subject and the data controller are allowed a period of twenty-one days in which to take action. See also Bainbridge *Data protection law* 132–135.

418 DP Act of 1998 s 12(8).

419 DP Act of 1998 s 12(9).

c Exempt decisions

The Act provides for exempt decisions where these provisions do not apply.[420] To qualify as an exempt decision two conditions must be met.[421] In the first place, either the decision must be taken in the context of a contract[422] or the decision must be authorised or required by or under any enactment.[423] In the second place, the effect of the decision must be to grant a request of the data subject, or (where the request is not granted) steps must have been taken to safeguard the legitimate interests of the data subject[424] (for example, by allowing him or her to make representations).[425] The Secretary of State may also prescribe by order other circumstances in which an automated decision may qualify as an exempt decision.[426]

4.3.5.5 Right to compensation

An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of the Act is, in terms of section 13 of the Act, entitled to compensation from the data controller for that damage.[427] The individual need not be the data subject affected by the processing. An individual is also entitled to compensation from the data controller for any distress suffered by

420 The exemptions are allowed by the Directive (Dir 95/46/EC a 15(2)).

421 DP Act of 1998 s 12(5).

422 More specifically, it must be taken in the course of steps taken for the purpose of considering whether to enter into a contract with the data subject, with a view to entering into such a contract, or in the course of performing such a contract (DP Act of 1998 s 12(6)(a)).

423 DP Act of 1998 s 12(6).

424 "Legitimate interests" is not defined, but Jay & Hamilton *Data protection* 213 suggest that they cover the right to respect for private life and family accorded under the European Convention on Human Rights, and the economic interests of the individual as a consumer and an employee.

425 DP Act of 1998 s 12(7). Chalton et al *Encyclopedia of data protection* par 1–246/4 argue that the operation of these provisions seems unnecessarily complex, which will create compliance uncertainties and procedural overheads for data controllers, while offering minimal effective protection for data subjects.

426 DP Act of 1998 s 12(5)(b). At the time of writing no such order has been proposed.

427 DP Act of 1998 s 13(1). This is required by the Directive (Dir 95/46/EC a 23(1)).

reason of such a contravention, but only if the individual also suffers damage,[428] or the contravention relates to the processing of personal data for so-called "special purposes".[429] The term "special purposes" refers to processing for journalistic, artistic or literary purposes.[430] It is a defence for a data controller against such proceedings to prove that he or she had taken such care as in all the circumstances was reasonably required to comply with the requirement in question.[431]

The court may also make a related order requiring the data controller to rectify, block, erase or destroy personal data, if it is satisfied that the data subject has suffered damage by reason of a contravention by a data controller of the requirements of the Act in circumstances entitling the data subject to compensation, and that there is a substantial risk of further contravention in respect of those data.[432]

4.3.5.6 Right to rectification, erasure or destruction of data

A data subject may apply for a court order requiring the data controller to rectify, block, erase or destroy such data relating to him or her as are inaccurate as well as any other personal data which

428 According to Chalton et al *Encyclopedia of data protection* par 1–248 it has been suggested that this provision may not comply with the Directive because the concept of "damage" has been interpreted too narrowly. The Data Protection Working Party (established under a 29 of the Directive – see ch 3 par 4.2.8.3) has stated that "'damage' in the sense of the data protection directive includes not only physical damage and financial loss, but also any psychological or moral harm caused (known as 'distress' under UK and US law" – see *Judging industry self-regulation* 5). The concept "damage" is not defined in the DP Act, but Jay & Hamilton *Data protection* 234 indicate that in general it would cover pecuniary loss such as loss of profits or earnings, and non-pecuniary loss such as pain and suffering and loss of amenity. Damages for pain and suffering depend on the individual's awareness of the pain (*Lim v Camden Health Authority* [1979] 2 All ER 910.) Damage may also consist of damage to reputation. In general, damages for distress are not recoverable save in those circumstances in which extreme distress which results in damage may count as actual damage, eg in cases of psychiatric injury. Damages are not awarded for shock, fear, anxiety or grief which are regarded as a normal consequence of a distressing event (*White v Chief Constable of Yorkshire* [1999] 1 All ER 1).

429 DP Act of 1998 s 13(2). In other words, where processing is for the special purposes, distress on its own will be a sufficient basis for a claim.

430 DP Act of 1998 s 3. See also par 4.3.6.2.e.

431 DP Act of 1998 s 13(3). Those circumstances would include matters such as the risk of possible damage to individuals and the extent of such damage (Jay & Hamilton *Data protection* 235).

432 DP Act of 1998 s 14(4). On rectification, erasure and destruction see par 4.3.5.6.

contain an expression of opinion which the court finds to be based on the inaccurate data.[433] Data are inaccurate if they are incorrect or misleading as to any matter of fact.[434] The concepts rectify, block, erase or destroy are not defined in the Act.[435]

Where the data, although inaccurate, accurately reflect information passed on by the data subject or a third party to the data controller, the court may, as an alternative to an order for rectification, blocking or destruction, take one of two further courses of action open to it. The first is to make an order requiring the data to be supplemented by a statement approved by the court of the true facts relating to the matters dealt with by the data. However, this course of action is only open to the court if certain requirements have been complied with.[436] These requirements are that (a) having regard to the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data, and (b) if the data subject has notified the data controller of the data subject's view that the data are inaccurate, the data indicate that fact. The second course of action open to the court, if these requirements have not been complied with, is to make such order as it thinks fit for securing compliance with those requirements with or without a further order requiring the data to be supplemented by such a statement.[437]

---

433 DP Act of 1998 s 14(1). The Directive seems to go further than the DP Act of 1998, because it provides that the right to seek rectification and erasure should extend to situations where incomplete data are processed (see Dir 95/46/EC a 12(b) and Chalton et al *Encyclopedia of data protection* par 1–264/1).

434 See DPR *Data Protection Act 1998* 20.

435 Jay & Hamilton *Data protection* 230–232 advance the following explanations for these terms: "Rectify" means to put a record straight. They suggest that the change made to the record should clearly indicate when and why the alteration was made in order to preserve an audit trail to show that the security requirements of the Act have been complied with. "Blocking" in the context of data processing means that the controller made the data inaccessible, although the data remains on the record. "Erasure" and "destruction" have the same effect, but they envisage different activities. Data are destroyed if the medium on which the data are held is physically destroyed. However, where the medium contains other data which are not inaccurate and should not be destroyed, the offending data should be removed by erasure, leaving the remainder of the record intact. Also see Bainbridge *Data protection law* 138.

436 These requirements are found in sch 1 part II par 7. This is the statutory interpretation of the fourth principle. See par 4.3.4.5.

437 DP Act of 1998 s 14(2).

As seen, the court may also make an order requiring the data controller to rectify, block, erase or destroy personal data, if it is satisfied that the data subject has suffered damage by reason of a contravention by a data controller of the requirements of the Act in circumstances entitling the data subject to compensation, and that there is a substantial risk of further contravention in respect of those data.[438]

In addition to an order that data must be rectified, blocked, erased or destroyed, the court may where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.[439] In determining whether it is reasonably practicable to require notification, the court must consider, in particular, the number of persons who would have to be notified.[440]

4.3.5.7 *Right to request Commissioner for assessment to be made as to whether any provision of Act has been contravened*

Any person (in other words, not only the data subject or an individual)[441] who believes himself or herself to be directly affected by any processing of personal data may ask the Commissioner to assess whether or not it is likely that the processing has been or is being carried out in compliance with the Act.[442] The

438 DP Act of 1998 s 14(4). The plaintiff does not have to bring an action for compensation in order to invoke this section (Jay & Hamilton *Data protection* 236).

439 DP Act of 1998 ss 14(3) and (5). The Directive requires that data subjects should have the right to obtain from data controllers notification to third parties, unless this is impossible or involves "a disproportionate effort" (Dir 95/46/EC a 12(c)). The DP Act of 1998 makes this right to notification of third parties subject to the discretion of the court, and "disproportionate effort" has become "reasonably practicable". This seems to be potentially non-compliant with the Directive. Also see Chalton et al *Encyclopedia of data protection* par 1–264/1.

440 DP Act of 1998 s 14(6).

441 A juristic person, such as a company or a trade union, will also in certain circumstances be able to make use of this right (Chalton et al *Encyclopedia of data protection* par 1–230/1).

442 Fromthe requirement that the person must be directly affected by the processing, it is evident that a person cannot use this provision as a general check. On the other hand, the request does not have to specify whether the person has any grounds for suspicion that the processing is being carried out in contravention of the Act (see also Jay & Hamilton *Data protection* 236).

request may also be made on behalf of such a person.[443] The Commissioner is obliged to carry out the assessment once a request has been received,[444] unless he or she has not been supplied with the information reasonably required to establish the identity of the person making the request, or to establish what form the processing in question took.[445]

The Act does not prescribe the manner in which the Commissioner should make the assessment, but lists the matters to which the Commissioner may have regard in deciding on the appropriate manner. They are the extent to which the request appears to raise a matter of substance, any undue delay in making the request, and whether or not the person making the request is entitled to make an application for access in respect of the personal data in question.[446]

The Commissioner only has a limited obligation to disclose the results of his or her consideration of the assessment. He or she must notify the person who made the request as to whether an assessment was made as a result of the request, and of any view formed or action taken as a result of the request.[447] However, the Commissioner does not have to provide information about the nature of the assessment, or state whether any further enquiries were undertaken, or provide any finding of fact or evidence.[448]

Depending on the Commissioner's assessment, this may lead to enforcement action being taken by the Commissioner pursuant to the complaint.[449] However, as Jay and Hamilton point out,[450] once a person has made a complaint to the Commissioner, the matter is out of the person's hands. It should also be

443 DP Act of 1998 s 42(1).

444 According to Chalton et al *Encyclopedia of data protection* par 1–231, the scope of this duty may significantly increase the Commissioner's workload.

445 DP Act of 1998 s 42(2).

446 DP Act of 1998 s 42(3).

447 DP Act of 1998 s 42(4).

448 See Jay & Hamilton *Data protection* 238.

449 See par 4.3.8.1.

450 Jay & Hamilton *Data protection* 238.

remembered that the Commissioner does not have the same powers as a court, for example he or she does not have the power to award compensation. Furthermore, the Commissioner has a regulatory function and while he or she may actively investigate an alleged breach, the Commissioner will not act on behalf of the complainant in the matter.[451] If the complainant is unhappy with the way in which the Commissioner is handling the case, the only recourse might be to seek judicial review.[452]

4.3.6 Exemptions

4.3.6.1 Introduction

There are a number of exemptions from various provisions of the Act provided for in part IV of the Act[453] and schedule 7 to the Act.[454] Those contained in part IV of the Act are referred to as "the primary exemptions", and those contained in schedule 7 are referred to as "the miscellaneous exemptions". In general, the primary exemptions are the ones which are either more likely to be claimed or which are more wide-ranging in terms of the scope of the exemption available.[455]

A general feature of the exemptions is that any exemption from the relevant provisions of the Act is available only in as much as compliance would prejudice the purpose governed by the exemption or if the particular exemption is required for the purpose concerned. In general the exemptions are not blanket exemptions,[456] but require a value judgment by the controller as to whether an exemption is

451 The Commissioner is only empowered to provide assistance to a complainant where data are processed for the "special purposes". See also par 4.3.6.2.e.

452 Jay & Hamilton *Data protection* 238.

453 DP Act of 1998 ss 28–36.

454 DP Act of 1998 sch 8 provides for transitional relief for exemptions that were available under the DP Act of 1984, but have been lost under the DP Act of 1998. These exemptions are manual data, processing otherwise than by reference to the data subject, payroll and accounts, unincorporated members' clubs and mailing lists, and back-up data. Also see Bainbridge & Pearce 1998 *Computer L & Sec Rep* 259, 264.

455 DPR *Data Protection Act 1998* 21.

456 Except for the national security exemption where personal data to be exempted may be identified by means (continued...)

available in a particular circumstance.[457] Most of the exemptions in the DP Act are based on an exemption allowed by the Directive. However, in some instances it appears that the DP Act allows broader exemptions than those envisaged by the Directive.[458]

The exemptions authorise non-compliance with various of the statute's provisions.[459] It is difficult to categorise the exemptions into classes which enjoy the same type of exemption. However, the Act contains two key phrases each of which refers to several of the provisions of the Act in respect of which an exemption might apply. These phrases are "subject information provisions" and "non-disclosure provisions". A number of categories of exemptions consist of an exemption from one or the other of these two groups of provisions.

The "subject information provisions" are defined as the first data protection principle in so far as this principle requires compliance with paragraph 2 of part II of schedule 1, and section 7.[460] The first data protection principle states that data should be processed fairly and lawfully, and the paragraph referred to requires that the data controller should, when the data are obtained, inform the data subject of the identity of the data controller and that of his or her representative, the purpose for which the data are intended to be processed and any further information which is necessary to enable the processing to be fair. This has been referred to as the "fair processing code".[461] Section 7 provides that data subjects have a right of access to their personal data. In other words, the subject information provisions are equivalent to the fair processing code (which requires data controllers to inform data subjects of various

456(...continued)
of a general description.

457 Bainbridge *Computer law* 408.

458 See fns 491, 534.

459 Carey *Data Protection Act 1998* 46. The exemption provisions contain detailed rules on how they will be applied in practice. I will not discuss every detail.

460 DP Act of 1998 s 27(2).

461 See par 4.3.4.2.

matters) and the subject access provisions.[462]

The Act gives the subject information provisions special status by providing that any other rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information, does not apply.[463] In other words, the subject access rights take precedence over other legal prohibitions on disclosure of information. The only restrictions that may exist are therefore the exemptions contained in the Act.[464]

The "non-disclosure provisions" are defined to mean the provisions specified in subsection 27(4) in so far as they are inconsistent with the disclosure in question.[465] The provisions specified in section 27(4) are:

- the first data protection principle, except in so far as it requires compliance with the conditions in schedules 2 and 3 (the conditions for processing and conditions for processing sensitive data)
- the second, third, fourth and fifth data protection principles,[466] and
- sections 10 (right to prevent processing likely to cause damage or distress) and 14(1) to (3) (right to rectification, blocking, erasure and destruction of incorrect data)

Exemption from the non-disclosure provisions is available in circumstances where the Act recognises that the public interest requires disclosure of personal data which would otherwise be in breach of the Act. Where an exemption from the non-disclosure provisions properly applies, such disclosure would not be in breach of the Act.[467]

---

462 DPR *Data Protection Act 1998* 21.

463 DP Act of 1998 s 27(5).

464 Carey *Data Protection Act 1998* 46; Chalton et al *Encyclopedia of data protection* par 1–201/1. Note specifically s 38(1) that empowers the Secretary of State to override s 27(5) (see text to fn 468).

465 DP Act of 1998 s 27(3).

466 For a discussion of the data protection principles, see par 4.3.4.

467 DPR *Data Protection Act 1998* 21.

Apart from the exemptions listed below, the Secretary of State may by order make further exemptions from the subject information provisions and non-disclosure provisions, if he or she considers it necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other individual.[468]

4.3.6.2 Primary exemptions

a National security[469]

The broadest exemption provided for in the Act can be claimed by a data controller where the exemption is necessary for the purpose of safeguarding national security. This exemption is in respect of all the mechanisms of control in the Act, namely any of the provisions of:

- the data protection principles[470]
- parts II (rights of data subjects),[471] III (notification by data controllers)[472] and V (enforcement)[473]
- section 55 (unlawful obtaining of personal data)[474]

468 DP Act of 1998 s 38. A draft of such an order, known as the Data Protection (Miscellaneous Subject Access Exemptions) Order of 1999, had been published. This draft order set out a number of legal provisions which prohibit or restrict the disclosure of information, and provide that where they apply the prohibitions takes precedence over the subject access rights in s 7. The legal provisions referred to include the Human Fertilisation and Embryology Act of 1990, and provisions relating to adoption records and papers. The Human Fertilisation and Embryology Act of 1990 exempts personal data which may show that a person was or might have been born as a result of treatment regulated under the Act.

469 DP Act of 1998 s 28(1). This exemption is allowed by the Directive (see Dir 95/46/EC a 13(1)(a)). Also see Bainbridge & Pearce 1998 *Computer L & Sec Rep* 180, 182.

470 See par 4.3.4.

471 See par 4.3.5.

472 See par 4.3.7.

473 See par 4.3.8.

474 See par 4.3.10.2.

The Act does not explain what would amount to "safeguarding national security" and a certificate of exemption, signed by a Minister of the Crown, is conclusive evidence that the requirements of the exemption have been met.[475] Such a certificate may identify the personal data by describing them in general terms[476] and may "be expressed to have prospective effect", in other words it may have effect at some time in the future.[477] Any person directly affected by the issuing of such a certificate may appeal to the Tribunal against the certificate.[478]

b Crime and taxation[479]

Processing for "crime and taxation purposes" refers to processing for the following purposes:

- the prevention or detection of crime
- the apprehension or prosecution of offenders
- the assessment or collection of any tax or duty or of any imposition of a similar nature[480]

The Act contains four categories of exemption which may be claimed under the crime and taxation heading. The first three may be claimed by any data controller who is able to fulfil the necessary conditions,[481] but the fourth category may be claimed only by the data controllers specified in the Act.

---

475 DP Act of 1998 s 28(2).

476 Eg, all "personal data held by the Home Office for the purpose of immigration" (see Jay & Hamilton *Data protection* 247).

477 DP Act of 1998 s 28(3).

478 DP Act of 1998 s 28(4). See par 4.3.9.2, 4.3.10.2. Also see DP Act of 1998 s 28(5)–(12) for further detailed provisions.

479 This exemption is allowed by the Directive (see Dir 95/46/EC a 13(1)(b)).

480 DP Act 1998 s 29(1).

481 Ie, the crime and taxation exemption is not limited to data held by the police or the Inland Revenue – any data controller may notify that data are held for these purposes (Chalton et al *Encyclopedia of data protection* par 1–2040).

Personal data processed for any purpose relating to crime and taxation are in the first instance exempt from both the first data protection principle (personal data are to be processed fairly and lawfully), except in so far as compliance is required with the conditions for processing and the conditions for processing sensitive data,[482] and subject access (section 7) in so far as the application of those provisions to the data would be likely to prejudice any purpose relating to crime and taxation.[483]

In the second place, personal data which are processed for the purpose of discharging statutory functions, and consist of information obtained for such a purpose from a person who had the data in his or her possession for any crime and taxation purposes, are exempt from the subject information provisions[484] in so far as the application of the subject information provisions to the data would be likely to prejudice any of the crime and taxation purposes.[485]

In the third place, personal data are exempt from the non-disclosure provisions[486] in any case where the disclosure is for any purpose relating to crime and taxation and where the application of those provisions in relation to the disclosure would be likely to prejudice any purpose relating to crime and taxation.

The Act does not explain the meaning of the phrase "likely to prejudice". The Commissioner takes the view that, for any of these three exemptions to apply, there would have to be a substantial chance rather than a mere risk that in a particular case the purposes would be notably prejudiced. The data controller needs to make a judgment as to whether or not prejudice is likely in relation to the circumstances of

482 In other words, the conditions for processing must still be complied with.

483 DP Act of 1998 s 29(1).

484 As seen, the subject information provisions can be paraphrased as meaning the fair processing code which requires data controllers to inform data subjects of various matters; and subject access. For a full description, see par 4.3.6.1.

485 DP Act of 1998 s 29(2).

486 As we have seen, the non-disclosure provisions refer to all the data protection principles except the security principle (principle 7), and some of the data subject rights. Where this exemption applies, it means *inter alia* that disclosures can be made even though it is unfair or incompatible with the original purpose. For a full explanation of the non-disclosure provisions, see par 4.3.6.1.

each individual case.[487]

The fourth exemption under the heading of crime and taxation can only be claimed by a data controller that is a government department, a local authority, or any other authority administering housing benefits or council tax benefits.[488] This exemption is further restricted to personal data that consist of a classification applied to the data subject as part of a system of risk assessment which is operated by the relevant authority[489] where such data are processed for any purpose relating to crime and taxation, but only in so far as the risk assessment relates to offences concerning fraudulent use of public funds, in addition to the assessment or collection of any tax or duty. Where the exemption applies, personal data are exempt from subject access in so far as such exemption is required in the interests of the operation of the system.[490]

c Health, education and social work[491]

Exemptions under this heading must be granted by the Secretary of State by order, and the exemptions

487 DPR *Data Protection Act 1998* 22.

488 DP Act of 1998 s 29(5).

489 The authority evaluates the risks of non-payment, non-compliance and fraud and attach risk markers to the particular records (Jay & Hamilton *Data protection* 250).

490 DP Act of 1998 s 29(4). If the authority were required to provide the risk markers attached to a particular record in response to a subject access request it might undermine the operation of the system (see Jay & Hamilton *Data protection* 250).

491 This exemption is **not** expressly allowed by the Directive. In fact, personal data relating to a person's physical and mental health are considered to be sensitive data, and the processing of such data is in general prohibited by the Directive (see Dir 95/46/EC a 8(1)). However, an exemption from this prohibition is allowed where the processing is for the purposes of preventive medicine, medical diagnosis, provision of care or treatment or the management of health-care services, provided that the person doing the processing is subject to a duty of confidentiality (Dir 95/46/EC a 8(3)). Further exemptions from the prohibition on processing may be laid down by national law or by decision of the supervisory authority, subject to suitable specific safeguards (Dir 95/46/EC a 8(4)). It is difficult to see on what grounds the DPA 1998 could grant an exemption from the subject information provisions in the case of health data. The only possible grounds would be Dir 95/46/EC a 13(1)(g) which provides that member states may adopt legislative measures to restrict the scope of the obligations and rights granted by certain provisions, including the provisions referred to as the subject information provisions in the DPA 1998, for the protection of the data subject and the rights and freedoms of others.

are from the subject information provisions.[492] The Secretary may also only modify those provisions. The following personal data may be exempted in this manner:

- personal data consisting of information as to the physical or mental health or condition of data subjects[493]
- personal data relating to present or past pupils of a school of which the data controller is the proprietor or teacher (as defined by the Act[494])[495]
- personal data processed by government departments or local authorities or by voluntary organisations or other bodies designated by the Secretary of State and which appear to them to be processed in the course of or for the purposes of carrying out social work in relation to the data subject or other individuals[496]

In the case of the social work exemption, there is a proviso in the Act that the Secretary of State may not grant any exemption or make any modification unless he or she considers that not to do so would be likely to prejudice the carrying out of social work.[497]

---

492 See par 4.3.6.1 for a description of the subject information provisions.

493 DP Act of 1998 s 30(1). This exemption will presumably be made applicable to situations where compliance with the exempted provisions would prejudice or damage the physical or mental health of the data subject, as was the case under the 1984 DP Act (Jay & Hamilton *Data protection* 257).

494 DP Act of 1998 s 30(5).

495 DP Act of 1998 s 30(2). Such an order, called the Data Protection (Subject Access Modification) (Education) Order 2000, came into effect in 2000. In terms of this order personal data may be exempt from subject access where the application of that right would be likely to cause serious harm to the physical or mental health of the data subject, or where it would otherwise be in the interests of the data subject that access should be withheld. For more detail, see Jay & Hamilton *Data protection* 262–263.

496 DP Act of 1998 s 30(3). Such an order, called the Data Protection (Subject Access Modification) (Social Work) Order 2000 came into effect in 2000. See http://www.homeoffice.gov.uk/ccpd/dpswsi.htm. In terms of this order personal data may be exempt from subject access where the application of that right would be likely to prejudice the carrying out of social work by reason of the fact that serious harm to the physical or mental health or condition of the data subject or any other person would be likely to be caused. For more detail, see Jay & Hamilton *Data protection* 258–259.

497 DP Act of 1998 s 30(3).

d Regulatory activity[498]

This exemption can be claimed by a range of bodies, since the exemption applies to personal data processed for a specific purpose, rather than to specific bodies or organisations. The exemption extends to personal data processed for the purposes of discharging the regulatory functions exercised by public "watch-dogs" which are all concerned with the protection of members of the public, charities or fair competition in business. The exemption is from the subject information provisions[499] in so far as the application of those provisions to the data would be likely to prejudice the proper discharge of those functions.[500]

Examples of such functions are those designed for protecting members of the public against financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned with the provision of banking, insurance, investment or other financial services or with the management of bodies corporate; or against financial loss due to the conduct of discharged or undischarged bankrupts or dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity;[501] or for protecting charities against misconduct or mismanagement in their administration.[502]

e Special purposes: journalism, literature and art

The DP Act of 1998 refers to processing for the purposes of journalism, artistic purposes, and literary

498 This exemption is allowed by the Directive (see Dir 95/46/EC a 13(1)(f)).

499 See text to fn 459 .

500 DP Act of 1998 s 31(1). For an interpretation of the phrase "likely to prejudice" see the crime and taxation exemption discussed above.

501 This exemption would eg cover the functions of the Law Society regulating the conduct of solicitors insofar as they are relevant to providing protection against malpractice, dishonesty or other seriously improper conduct (Jay & Hamilton *Data protection* 251).

502 DP Act of 1998 s 31(2). Also see s 31(3)–(5) for more details.

purposes as data processing for "the special purposes".[503] The exemption of processing for the special purposes is a new exemption in the DP Act of 1998, and is a result of the Directive which requires of EU member states to provide for exemptions for processing of personal data in the interests of freedom of expression.[504] In the DP Act of 1998, freedom of expression has been thus been equated with three particular areas of activity, namely journalism, artistic and literary work, and no other activity will enjoy the benefit of the freedom of expression exemption.[505]

The Act stipulates four conditions which must be present before the processing of personal data for the special purposes can qualify for exemption from a number of provisions of the Act, namely that:

- the personal data are processed only for the special purposes
- the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material
- the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest
- the data controller reasonably believes that, in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the special purposes[506]

503 DP Act of 1998 s 3. Apart from providing an exemption for processing for the special purposes, the Act also constrains the Commissioner's powers of enforcement when processing of personal information takes place for these purposes. See par 4.3.8.

504 Dir 95/46/EC a 9. As seen (ch 3 par 4.2.4.4), Britain was in principle opposed to the inclusion of such a provision in the Directive. Chalton et al *Encyclopedia of data protection* par 1–199/2 call the special purposes exemption the "most significant new exemption" in the Act. Apparently the publication of the Data Protection Bill was much delayed in order to resolve press interests. The resulting provisions are, according to Jay & Hamilton *Data protection* 265, "ones of extraordinary complexity". They caution that "[t]he individual data subject who seeks to take on the media will find himself facing a daunting task". According to these authors (on 265–266), "[i]t is not simply that the provisions are complex, but that the shifts in responsibility and in the burden of proof in crucial points in the proceedings together with the multiple possible adjudications and appeals before a final disposal of the case will make the case difficult to conclude. However wronged they may feel, individuals may be best advised not to embark on these proceedings unless they have deep pockets, considerable resilience, and a favourable life expectancy".

505 Jay & Hamilton *Data protection* 265.

506 DP Act of 1998 s 32(1).

All of these requirements are subject to interpretation, and since they represent a new provision in UK law, there is no authority under the 1984 Act to rely on. Regarding the requirement that the processing should be only for the specified special purposes, the recommendations of the Data Protection Working Party should be noted.[507] These recommendations emphasise that exemptions may cover only data processing for journalistic (editorial) purposes, and that any other form of data processing by journalists or the media (for example data processing for billing purposes) is subject to the ordinary rules of data protection.[508] At the same time is should be noted that the exemptions are not granted to the media or journalists as such, but to anybody processing personal data for journalistic purposes. On the requirement that the processing should take place with a view to publication, the Act provides that "publish" means "in relation to journalistic, literary or artistic material ... [to] make available to the public or any section of the public".[509] According to the Data protection Working Party, publication includes electronic publishing.[510] The last two requirements reflect that this exemption requires a balance to be struck between freedom of expression on the one hand and privacy of individuals on the other hand, and that an exemption in favour of freedom of expression is only mandatory in so far as it is necessary to strike the correct balance.[511] In considering whether the belief of a data controller that publication would be in the public interest was or is a reasonable one, regard may be had to his or her compliance with any code of practice which is relevant to the publication in question, and is designated by the Secretary of State by order for the current purposes.[512]

The exemption available is from the data protection principles (except the seventh data protection principle which concerns security measures) and the individual rights-provisions (subject access –

507 The Working Party was established under a 29 of the Directive (see ch 3 par 4.2.8.3).

508 Data Protection Working Party *Data protection law and the media* 8.

509 DP Act of 1998 s 32(6).

510 Data Protection Working Party *Data protection law and the media* 8.

511 According to the Data Protection Working Party *Data protection law and the media* 7, in striking this balance cognisance can also be taken of rules which, although not part of the data protection legislation in a proper sense, still contribute to the protection of the privacy of individuals. Such rules include the rules concerning libel and the professional obligations of journalists.

512 DP Act of 1998 s 32(3).

section 7; right to prevent processing likely to cause damage or distress – section 10; rights in relation to automated decision-taking – section 12; provisions relating to rectification, blocking, erasure and destruction of inaccurate data – section 14 (1) to (3)).[513]

If the controller reasonably believes that the publication is in the public interest and that compliance with the data protection principle in respect of which the exemption is claimed is incompatible with publication, he or she could disregard the principle, for example he or she could disregard the prohibition on sensitive data holding, the requirement for legitimacy of processing and the prohibition on overseas transfer.[514]

Whereas exemption from the data protection principles is claimed proactively, exemption from the individual rights provisions is claimed reactively when individuals seek to exercise the relevant right. If a person brings proceedings against a data controller to enforce his or her rights under the Act before publication of the work in question, the data controller can insist that the proceedings should be halted until the Commissioner has made a declaration that the processing is no longer being carried out for the special purposes. This in effect allows the data controller to stay the proceedings until after the publication of the relevant material.[515]

The court is obliged to stay the proceedings until either of two conditions are met.[516] These conditions are (i) that a determination of the Commissioner under section 45 with respect to the data in question has taken effect, or (ii) in a case where the proceedings were stayed on the making of a claim, that the

513 DP Act of 1998 s 32(2). The Directive allows exemptions from the general rules on lawfulness of the processing of personal data, the rules on transfer of data to third countries and the rules on the supervisory authority. However, there may be no exemptions from the security principle. The supervisory authority must also have *ex post* powers, eg to publish a regular report or to refer matters to judicial authority (see Dir 95/46/EC recitals par (37)).

514 Jay & Hamilton *Data protection* 271.

515 As stated previously, the policy behind these exemptions is to protect freedom of expression. The provisions intend to prevent prior restraint of publications and aim to ensure that data protection principles are not used to stifle freedom of the press when exercised in the public interest (see Jay & Hamilton *Data protection* 272).

516 DP Act of 1998 s 32(4).

claim has been withdrawn.[517]

Section 45 provides that where it appears to the Commissioner at any time that personal data are not being processed only for the special purposes, or are not being processed with a view to the publication by a person of journalistic, literary or artistic material which has not previously been published by the data controller, he or she may make a determination in writing to that effect.[518] The Commissioner may therefore lift the stay on the court proceedings where he or she is able to make a determination to that effect, otherwise the stay will continue to apply.[519] However, the person processing for the special purposes may delay the process further, because there is a right of appeal against this determination.[520]

There are also special provisions affecting the Commissioner's power to deal with personal data processed for the special purposes. These will be discussed under the enforcement powers of the Commissioner.[521]

f Research, history and statistics

As noted previously, the Directive accords special treatment to data processing for statistical, historic or scientific uses.[522] The DP Act of 1998 therefore also provides for various exemptions in respect of the processing (or further processing) of personal data for research purposes, which are broadly defined as including statistical or historical purposes.[523] Any research, whether carried out in the public

517 DP Act of 1998 s 32(5).

518 DP Act of 1998 s 45(1).

519 Jay & Hamilton *Data protection* 274.

520 DP Act of 1998 s 48. Note that a determination by the Commissioner as to the special purposes may be made at any time and not just in the above circumstances or as a result of the service of a special information notice (DP Act of 1998 s 45(1)).

521 See par 4.3.8.

522 See ch 3 par 4.2.4.1.

523 DP Act of 1998 s 33(1).

or private sector, whether commercial or academic, can claim one or more of the exemptions as long as it processes personal data only for research purposes and fulfils the safeguard conditions for the exemption.[524] The safeguard conditions, both of which have to be met, are:

- The data must not be processed to support measures or decisions with respect to particular individuals.[525]

- The data must not be processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.[526]

If the safeguard conditions are met:

- The further processing of personal data for research purposes will not be considered incompatible with the purposes for which they were originally obtained (this is an exemption from the second data protection principle).[527]

  Note that this exemption does not excuse the data controller from complying with that part of the second data protection principle which states that personal data may be obtained only for one or more specified and lawful purpose.[528] The use of data for research therefore does not in itself constitute a legitimate condition for processing personal data. The researcher will have to rely on another condition, for example that the data subject has consented to the processing, or that the processing is necessary for the purpose of legitimate interests pursued by the data

524 Jay & Hamilton *Data protection* 281.

525 The prohibition is aimed at the use of particular personal data, not the use of the results of the research. Research leading to statistical findings, eg that a particular drug has positive effects on a particular type of patient, which findings are then used as a basis for making decisions in individual cases, falls within the exemption (Jay & Hamilton *Data protection* 288).

526 DP Act of 1998 s 33(1).

527 DP Act of 1998 s 33(2). See par 4.3.4.3 regarding the second data protection principle.

528 DPR *Data Protection Act 1998* 24.

controller or by the third party to whom the data are disclosed.[529]

- Personal data can be kept indefinitely for research purposes despite the fifth data protection principle.[530]

- Subject access (section 7) does not have to be given provided that the results of the research or any resulting statistics are not made available in a form which identifies data subjects.[531]

The Act sets out a list of disclosures of personal data that may be made without risking the loss of the research exemption. These cover disclosures:

- to any person, for research purposes only
- to the data subject or someone acting on his or her behalf
- at the request, or with the consent, of the data subject or someone acting on his or her behalf
- where the person making the disclosure has reasonable grounds for believing the disclosure falls within one of the above[532]

As noted previously, sensitive data may be used for medical research, provided that the processing is necessary for medical purposes and is undertaken by a health professional, or a person who in the circumstances owes a duty of confidentiality to the data subject which is equivalent to that which would arise if that person were a health professional.[533]

---

529 Jay & Hamilton*Data protection* 284–285. On the conditions for processing personal data, see par 4.3.4.2.b.

530 DP Act of 1998 s 33(3).

531 DP Act of 1998 s 33(4).

532 DP Act of 1998 s 33(5).

533 DP Act of 1998 sch 3 par 8(1). As noted previously, the Directive's definition of medical purposes does not include medical research and this has been a controversial addition to the Act by the UK government (see fn 278).

g Publicly available information[534]

When personal data consist of information which the data controller is obliged by or under any enactment to make available to the public (whether by publishing it, or by making it available for inspection, or otherwise, and whether gratuitously or on payment of a fee), then personal data are exempt from:[535]

- ❒ the subject information provisions[536]
- ❒ the fourth data protection principle (which relates to accuracy)[537]
- ❒ section 14(1) to (3) (rectification, blocking, erasure and destruction of incorrect data)
- ❒ the non-disclosure provisions[538]

This is a broad exemption, but it may only be claimed by a data controller who is under an obligation to make the information public. It does not apply once the information has passed on into the hands of another party.[539]

There is also no requirement to notify where the sole purpose of any processing is the maintenance of

534 The Directive, to my mind, does not provide for this exemption. The only exemption that exists in the Directive for public registers set up by law is from the requirement that the data controller should notify the data protection authority before any processing of data takes place (see Dir 95/46/EC a 18(3)).

535 DP Act of 1998 s 34.

536 See fn 459.

537 Under the DP Act of 1984 data which were already publicly available by law were generally exempted from the provisions of the Act. The Registrar (Fifth Report 1989 part B para 227) recommended that the exemption be modified to reduce it from a general exemption to a non-disclosure exemption, arguing that the data user should not be released from all the principles, eg the principle of accuracy, merely because he or she has to publish the information (see also Chalton et al *Encyclopedia of data protection* par 1–199). This recommendation was not accommodated in the new Act.

538 See fn 464.

539 Jay & Hamilton *Data protection* 298.

a public register.[540]

h Legal exemptions[541]

Personal data are exempt from the non-disclosure provisions[542] where the disclosure is mandatory, because it is required by or under any enactment, by any rule of law or by the order of a court,[543] or where the disclosure is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or for the purpose of obtaining legal advice, or as is otherwise necessary for the purposes of establishing, exercising or defending legal rights.[544]

Under the miscellaneous exemptions,[545] two exemptions are found that could also be grouped under the heading of legal exemptions, namely an exemption for legal professional privilege and one to prevent self-incrimination: Personal data are exempt from the subject information provisions if the data consist of information in respect of which a claim to legal professional privilege or, in Scotland, to confidentiality as between client and professional legal adviser, could be maintained in legal proceedings.[546] A person need not comply with a subject access request where compliance would, by revealing evidence of the

540 See par 4.3.7 on notification. Also see fn 534.

541 The Directive does not expressly allow this exemption, but it could be based on Dir 95/46/EC a 13(1)(g) (see fn 491).

542 See fn 464.

543 DP Act of 1998 s 35(1). This exemption would eg covers disclosures which an employer is required to make to the Inland Revenue by the statutory provisions which govern that department (see DPR *Guidelines* 100). Also relevant in this regard is the Public Interest Disclosure Act of 1998 which is designed to protect individuals who make certain disclosures of information in the public interest (ie "whistle blowers"). See Chalton et al *Encyclopedia of data protection* par 1–223/1 for an analysis of the way this Act and the DP Act of 1998 will relate to each other.

544 DP Act of 1998 s 35(2). This exemption would apply eg when a party to a legal proceeding makes a disclosure (DPR *Guidelines* 100).

545 See par 4.3.6.3.

546 DP Act of 1998 sch 7 par 10. For a discussion of legal professional privilege in the UK (in Scotland referred to as confidentiality between client and professional legal adviser), see Chalton et al *Encyclopedia of data protection* par 1–209 – 1–211.

commission of any offence other than an offence under the DP Act of 1998, expose him or her to proceedings for that offence.[547] Although a person may not refuse to comply with a subject access request merely because this would involve revealing evidence of an offence under the DP Act, that evidence would not be admissible against the person in relation to proceedings under this Act.[548]

i Domestic purposes

The Directive provides that its provisions are not applicable to the processing of personal data by a natural person in the course of a purely personal or household activity.[549] The DP Act of 1998 consequently exempts personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes) from the data protection principles and the provisions of parts II (individual rights) and III (notification).[550] This is a wide-ranging exemption, but it does not extend to part V of the Act, which deals with enforcement by the Commissioner.[551]

4.3.6.3 Miscellaneous exemptions[552]

The miscellaneous exemptions provided for by the Act are situations where data controllers are exempted either from the subject access provision of section 7 or from the subject information

547 DP Act of 1998 sch 7 par 11(1).

548 DP Act of 1998 sch 7 par 11(2). Also see Chalton et al *Encyclopedia of data protection* par 1–217/1.

549 Dir 95/46/EC a 3(2).

550 DP Act of 1998 s 36.

551 DPR *Data Protection Act 1998* 25.

552 None of these exemptions found in DP Act of 1998 sch 7 is expressly provided for by the Directive; presumably they are all based on Dir 95/46/EC a 13(1)(g) which provides that member states may adopt legislative measure to restrict the scope of the obligations and rights granted by certain provisions, for the protection of the data subject and the rights and freedoms of others. Bainbridge & Pearce 1998 *Computer L & Sec Rep* 180, 182 also think that the DP Act of 1998 goes further than the Directive in respect of the exemptions.

provisions.[553]

a Armed forces

A new exemption in the Act is that personal data are exempt from the subject information provisions in any case where the application of those provisions would be likely to prejudice the combat effectiveness of any of the armed forces of the Crown.[554]

b Judicial and Crown appointments and Crown employment

Personal data processed for the purposes of assessing any person's suitability for judicial office or the office of Queen's Counsel, or the conferring by the Crown of any honour, are exempt from the subject information provisions.[555] This exemption can be claimed by any data controller that processes personal data for these purposes. The exemption is absolute in the sense that it does not have to be considered on a case by case basis, nor does it only apply to the extent of any incompatibility.[556]

The Secretary of State may by order exempt from the subject information provisions personal data processed for the purposes of assessing any person's suitability for employment by or under the Crown, or any office to which appointments are made by Her Majesty, by a Minister of the Crown or by a Northern Ireland department.[557]

c Business and corporate finance exemptions: Confidential references given by data controller, management forecasts, corporate finance,

553 On the subject information provisions, see text to fn 459.

554 DP Act of 1998 sch 7 par 2. Bainbridge *Data protection law* 185–186 discusses situations where this exemption could fall foul of the Human Rights Act of 1998.

555 DP Act of 1998 sch 7 par 3.

556 Jay & Hamilton *Data protection* 297.

557 DP Act of 1998 sch 7 par 4.

negotiations

A new exemption in the DP Act of 1998 is that personal data are exempt from the subject access provision if they consist of a reference given or to be given in confidence by the data controller for the purposes of the education, training, employment or appointment to any office of the data subject, or the provision of any service by the data subject.[558] This exemption is not available for such references where they are not given in confidence or where they are received (ie not given) by the data controller.[559]

In so far as the application of any of the subject information provisions to personal data processed for the purposes of management forecasting or management planning would be likely to prejudice the conduct of the business or other activity of the data controller, such personal data are exempt from the subject information provisions.[560] This exemption is available to businesses to protect the confidentiality of personal data processed for the above-mentioned purposes.[561]

The DP Act also provides for an exemption from the subject information provisions of personal data processed for the purposes of, or in connection with, "a corporate finance service" (as defined in the

558 DP Act of 1998 sch 7 par 1. Note that this exemption refers to references given for purposes of education, training, employment or appointment – it does not include credit references. Also see Singleton *Data protection* 52. For the effect of this provision on "indications of intention", see fn 136. A letter of reference that does not form part of a relevant filing system, will in any case be outside the scope of the Act (Bainbridge *Data protection law* 185).

559 DPR *Data Protection Act 1998* 25; Chalton et al *Encyclopedia of data protection* par 1–217/1.

560 DP Act of 1998 sch 7 par 5.

561 DPR *Data Protection Act 1998* 25. Also refer to fn 136 for the effect of this exemption on "indications of intention".

Act)[562] provided by "a relevant person" (as defined in the Act).[563] The exemption is only available in so far as the application of the subject information provisions could, or in the reasonable belief of the data controller could, affect the price or value of particular instruments of a price-sensitive nature.[564]

The exemption is also available if required for the purpose of safeguarding an important economic or financial interest of the United Kingdom (subject to an order by the Secretary of State clarifying when and in what circumstances such an exemption is available).[565]

Personal data which consist of records of the intentions of the data controller in relation to negotiations with the data subject are exempt from the subject information provisions in so far as the application of those provisions would be likely to prejudice those negotiations.[566]

---

562 DP Act of 1998 sch 7 par 6(3) defines "corporate finance service" as "a service consisting in–
(a) underwriting in respect of issues of, or the placing of issues of, any instrument,
(b) advice to undertakings on capital structure, industrial strategy and related matters and advice and service relating to mergers and the purchase of undertakings, or
(c) services relating to such underwriting as is mentioned in paragraph (a)".

563 DP Act of 1998 sch 7 par 6(3) defines "relevant person" as "meaning –
(a) any person who is authorised under Chapter III of part I of the Financial Services Act of 1986 or is an exempted person under Chapter IV of part I of that Act,
(b) any person who, but for part III or IV of schedule 1 to that Act, would require authorisation under that Act,
(c) any European investment firm within the meaning given by Regulation 3 of the Investment Services Regulations of 1995,
(d) any person who, in the course of his employment, provides to his employer a service falling within paragraph (b) or (c) of the definition of "corporate finance service", or
(e) any partner who provides to other partners in the partnership a service falling within either of those paragraphs".

564 DP Act of 1998 sch 7 par 6(1). Jay & Hamilton *Data protection* 294 give an example of how this applies: An adviser (falling within the definition of "a relevant purpose") who is working for a company which is considering a bid for another undertaking carries out enquiries into the directors of the target undertaking. If those enquiries were to become known, via a response to a subject access request, this could trigger price movements in the shares in the target company.

565 DP Act of 1998 sch 7 par 6(2). The Directive expressly allows for exemptions to safeguard an important economic or financial interest of a member state of the European Union (Dir 95/46/EC a 13(1)(e)).

566 DP Act of 1998 sch 7 par 7. Also refer to fn 136 for the effect of this exemption on "indications of intention".

d Educational exemptions: Examination marks and examination scripts

This is not an exemption as such but an adaptation of the requirements of section 7 of the Act that a subject access request must be complied with within a specified period of time (forty days from receipt of the request or, if later, receipt of the information required to comply with the request and the fee).[567] Where a subject access request is made in relation to examination marks or results,[568] before the examination results are announced, the time scale is extended to either five months from the day on which the data controller received the request (or, if this period is exceeded, from the first day on which the data controller has both the required fee and the information necessary to act on the request), or forty days from the announcement of the examination results,[569] whichever is the earlier.[570] The provision is designed to stop students jumping the queue to obtain the results of examinations earlier than they would do in the normal scheme of things.[571]

Personal data consisting of information recorded by candidates during an academic, professional or other examination are exempt from the subject access provisions of section 7.[572]

4.3.7 Notification by data controllers

The Directive makes it incumbent on member states to require the data controllers, or their

567 DPR *Data Protection Act 1998* 26.

568 DP Act of 1998 sch 7 par 8(1). "Examination" is defined in DP Act of 1998 sch 7 par 8(5) as "including any process for determining the knowledge, intelligence, skill or ability of a candidate by reference to his performance in any test, work or other activity". According to Jay & Hamilton *Data protection* 297 the exemption appears to apply to data consisting of actual marks and marking schemes and to data processed as a result of the determination of the results, such as the pass mark, the rankings, and any remarking.

569 According to DP Act of 1998 sch 7 par 8(4) the results of an examination must be treated as having been announced when they are first published or (if not published) when they are first made available or communicated to the candidate in question.

570 DP Act of 1998 sch 7 par 8(2).

571 Jay & Hamilton *Data protection* 297.

572 DP Act of 1998 sch 7 par 9.

representatives, to furnish certain information to the supervisory authority, to require that prior checking of certain processing operations be done on the basis of this information, and that this information be published in a register of processing operations.[573]

Giving effect to the Directive, the DP Act of 1998 replaces the registration system that existed under the DP Act of 1984 with a notification system.[574] As has been said, the concept of mandatory registration of data users was a central recommendation of the Lindop Committee, and this was reflected in the 1984 Act. At the time when the Lindop Committee was functioning, computing was confined to a few large organisations, and registration of all data users was an attainable object. However, the availability of the personal computer during the 1980s changed all of this. By the 1990s the registration system came to be considered as "burdensome, bureaucratic and unnecessarily detailed".[575] Under the 1998 Act, the primary purpose of notification is "to promote transparency" of data processing.[576] Under the 1998 DP Act, the Data Protection Registrar becomes the Commissioner, which reflects the changing nature of the post.[577]

4.3.7.1 Duty to notify

The DP Act provides that no processing of personal data may take place unless an entry in respect of the data controller is included in a register maintained by the Commissioner.[578] It is an offence to

573 Dir 95/46/EC aa 19–21.

574 The DP Act of 1998 contains provisions dealing with the transition from registration to notification (DP Act of 1998 sch 14). The Act does not work out all the details of the notification procedure. The Secretary of State will make notification regulations after receiving proposals in this regard from the Commissioner (see DP Act of 1998 s 25).

575 Jay & Hamilton *Data protection* 135.

576 See Home Office Consultation Paper *Subordinate legislation: notification regulations* (1998) quoted in Jay & Hamilton *Data protection* 136.

577 DP Act of 1998 s 6(1). As from 30 January 2000 the Data Protection Commissioner was known as the Information Commissioner. See also fn 107.

578 DP Act of 1998 s 17(1).

process personal data without notification,[579] unless the processing is exempt from notification.[580] The Act does not provide for a defence to this offence, and liability is therefore strict.[581]

4.3.7.2 Information to be provided

Any data controller who wishes to be included in the register maintained by the Commissioner is obliged to submit a notification to the Commissioner.[582] The Commissioner may no longer refuse to place an entry on the register, as long it is made in the proper form.[583] The notification must specify what the Act calls "the registrable particulars" as well as a general description of the security measures taken to protect the personal data.[584] The information relating to security measures must be notified, but will not appear on the register. The information to be notified covers the data, the purposes of processing, data subjects, recipients, and overseas transfers. The sources of the data need not be notified.[585]

The "registrable particulars" refer to the following information:[586]

- the name and address of the data controller
- the name and address of any representative of the data controller
- a description of the personal data being processed
- a description of the category or categories of data subjects to which the data relate

579 DP Act of 1998 s 21(1).

580 See par 4.3.7.3.

581 See DPR *Data Protection Act 1998* 42.

582 DP Act of 1998 s 18(1).

583 Jay & Hamilton *Data protection* 143. The Commissioner may eg not refuse to add a data controller to the register solely on the grounds that processing will not comply with the data protection principles. However, if the processing proceeds in contravention of the law, the Commissioner may exercise his or her enforcement powers (see Bainbridge & Pearce 1998 *Computer L & Sec Rep* 180, 181 fn 5).

584 DP Act of 1998 s 18(2).

585 Jay & Hamilton *Data protection* 136.

586 DP Act of 1998 s 16(1).

- a description of the purpose or purposes for which the data are being or are to be processed
- a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data[587]
- the names, or a description of, any countries or territories outside the EEA[588] to which the data controller directly or indirectly transfers, or intends to transfer, the data
- in any case where personal data are being, or are intended to be, processed in circumstances in which the prohibition against processing without notification is excluded,[589] and the notification does not extend to those data, a statement of that fact.[590]

The notification must be accompanied by a fee prescribed by regulation made by the Secretary of State.[591] The notification regulations must also include provisions imposing on data controllers in respect of whom an entry is included in the register a duty to notify to the Commissioner of changes in the registrable particulars and the measures taken to comply with the security principle.[592] It is an offence to fail to comply with this duty,[593] but it will be a defence to persons charged with such an offence that they exercised all due diligence to comply with the duty.[594]

---

587 For the definition of recipients, see text to fn 177.

588 See fn 160 on the members of the EEA.

589 See par 4.3.7.3.

590 This provision reflects the fact that not all personal data have to be included in the register: eg as a general rule manual data need not be included (see par 4.3.7.3). Data controllers may choose to include any of these categories of exempt data in their register entries on a voluntary basis, but if they decide not to include them, their entries must state that they have not done so.

591 DP Act of 1998 s 18(5). The Secretary of State may, *inter alia*, also prescribe by regulation the form in which the particulars must be given (see DP Act of 1998 s 18(3) and also see s 18(4) for other aspects on which regulations may be made). The Secretary of State may also make regulations regarding fees, prescribing the fees that are payable in certain prescribed situations (DP Act of 1998 s 26).

592 DP Act of 1998 s 20.

593 DP Act of 1998 ss 21(1).

594 DP Act of 1998 ss 21(2) and (3).

4.3.7.3 Exemptions from notification

As allowed by the Directive,[595] the DP Act of 1998 provides in certain circumstances for exemptions from the notification requirement.[596] As stated previously, notification is not a control mechanism and the Commissioner cannot refuse a notification. Equally important to note is that an exemption from notification confers no other exemptions. Controllers who are exempt from processing must still be able to provide an enquirer with the equivalent information to that contained in the register. Voluntary notification will be allowed if the controllers wish to have a public statement available.[597]

The notification requirement is in the first instance not applicable in relation to personal data that are not processed automatically, that is data consisting of information which is either "part of a relevant filing system" or which is part of an "accessible record".[598] However, if the processing of such exempted data is considered to be "assessable processing" (which must be notified to the Commissioner before commencement of the processing to allow the Commissioner to make an assessment of it because it poses a risk of damage or injury to data subjects)[599] the exemption does not apply.[600] In other words, manually processed data need not be notified, unless they fall into an assessable processing category.

The notification requirement may also be excluded by the Secretary of State by regulation if it appears that processing of a particular description is unlikely to prejudice the rights and freedoms of data

595 Dir 95/46/EC aa 18(2)–(5).

596 Under the DP Act of 1984 the Registrar could not enforce the data protection principles against those users that were exempted from the registration requirement. This position has now changed, and the Commissioner may enforce the principles against data controllers exempted from notification. See also par 4.2.1.7 and Singleton *Data protection* 41.

597 Jay & Hamilton *Data protection* 136. Also see fn 590.

598 DP Act of 1998 s 1(1). See par 4.3.3.1.a. Although manual processing is exempt from notification, the processor may choose to notify such processing. If processing is not notified, the data controller must be prepared to make available the information that would have been in the registrable particulars to any person on request (see also par 4.3.7.5 and see Bainbridge *Data protection law* 67; Bainbridge & Pearce 1998 *Computer L & Sec Rep* 180, 181; 1998 *Computer L & Sec Rep* 259, 260).

599 See par 4.3.7.7.

600 DP Act of 1998 s 17(2).

subjects.[601]

The notification requirement also does not apply in relation to any processing whose sole purpose is the maintenance of a public register,[602] or where processing is within the national security exemption or the domestic purposes general exemption.[603]

4.3.7.4 Data protection supervisors

The Directive provides that the notification procedure may also be simplified or exempted where the controller appoints a personal data protection official who is responsible for ensuring, in an independent manner, the internal application of the national provisions taken pursuant to the Directive, and who is responsible for keeping the register of processing operations carried out by the controller.[604] The Secretary of State must by order establish the conditions under which data controllers may appoint a person to act as a data protection supervisor.[605] Such an order will simplify the notification provisions for those controllers who appointed data protection supervisors. A particular responsibility of the data protection supervisor is the independent monitoring of the data controller's compliance with the provisions of the DP Act of 1998.[606] The order may impose duties on data protection supervisors in relation to the Commissioner, and confer functions on the Commissioner in relation to data protection supervisors.[607]

601 DP Act of 1998 s 17(3).

602 DP Act of 1998 s 17(4).

603 See par 4.3.6.2 and Chalton et al *Encyclopedia of data protection* par 1–142/4.

604 Dir 95/46/EC art 18(2).

605 This provision would appear to give the Commissioner the power to impose upon a company the appointment of an independent data protection compliance officer (Mullock & Leigh-Pollitt *Data Protection Act explained* 45).

606 DP Act of 1998 s 23(1).

607 DP Act of 1998 s 23(2).

4.3.7.5 Duty of data controller to make information available

The data controllers who are exempted from notification are nevertheless under an obligation to provide the same information as is contained in the registrable particulars,[608] free of charge, within twenty-one days of receiving a written request for such particulars from any person.[609] Data controllers who fail to comply with this duty are guilty of an offence,[610] unless they can show that they exercised all due diligence to comply with the duty.[611]

4.3.7.6 Register of notifications

The Commissioner is obliged to maintain a register of persons who have given notification and make an entry in the register in pursuance of each notification received from a person in respect of whom no entry as data controller had hitherto been included in the register.[612]

Each entry in the register must consist of the registrable particulars as notified or as amended, and such other information as the Commissioner may be authorised or required by notification regulations to include in the register.[613] No entry may be retained in the register for more than twelve months or such other period as is prescribed by notification regulations.[614]

The Commissioner is to provide facilities for making the information contained in the entries in the register available for inspection (in visible and legible form) by members of the public at all reasonable

608 See text to fn 586.

609 DP Act of 1998 s 24(1).

610 DP Act of 1998 s 24(4).

611 DP Act of 1998 s 24(5).

612 DP Act of 1998 s 19(1).

613 DP Act of 1998 s 19(2).

614 DP Act of 1998 ss 19(4) and (5).

hours and free of charge. The Commissioner may also provide for other facilities to make such information available to the public.[615] The Commissioner is also obliged to supply members of the public with a certified written copy of the particulars contained in any entry made in the register, upon payment of a fee if a fee is prescribed by regulation.[616]

4.3.7.7 Preliminary assessment by Commissioner

The notification process enables the supervisory authority to carry out prior checks on processing operations likely to present specific risks to the rights and freedoms of data subjects.[617] In this regard the DP Act of 1998 introduces "assessable processing" provisions in respect of any processing of a description specified in an order made by the Secretary of State as being particularly likely to cause substantial damage or substantial distress to data subjects or otherwise significantly to prejudice the rights and freedoms of data subjects.[618] It is not yet known exactly what types of processing will be subject to these provisions as no order has been made specifying this.[619] However, there appears to be three possible categories that may be subject to preliminary assessment either generally or in certain areas, namely:

- ❒ data matching
- ❒ processing involving genetic data
- ❒ processing by private investigators[620]

On receiving notification from a data controller, the Commissioner is obliged to consider whether the processing that is the subject of the notification is assessable processing and, if so, whether or not the

615 DP Act of 1998 s 19(6).

616 DP Act of 1998 s 19(7).

617 See Dir 95/46/EC art 20(1).

618 DP Act of 1998 s 22(1). The Directive does not specifically mention damage or distress (see Bainbridge & Pearce 1998 *Computer L & Sec Rep* 259, 260).

619 DPR *Data Protection Act 1998* 42.

620 DPR *Data Protection Act 1998* 39.

assessable processing is likely to comply with the provisions of the Act.[621] The Commissioner has twenty-eight days to give a notice to the data controller stating the extent to which the Commissioner is of the opinion that the processing is likely or unlikely to comply with the provisions of this Act.[622]

Upon making a notification involving assessable processing to the Commissioner, the data controller is initially subject to an absolute prohibition on assessable processing, until either the period given to the Commissioner in which to make the consideration has lapsed or, before the end of that period, the data controller has received a notice from the Commissioner.[623] A contravention of this prohibition is an offence.[624]

Lloyd, commenting on this provision, points out that should the Commissioner's assessment be that the processing would be unacceptable, there would not appear to be any mechanism to prevent the data controller continuing with the plans although it might be expected that an enforcement notice would be served in this event.[625] Jay and Hamilton agree that the "assessable processing provisions ... cannot be used to ignite the Commissioner's enforcement powers".[626] However, if the Commissioner were free to inform individuals who are potentially affected by the assessable processing of the imminent risks, this would enable the individuals to lodge notices of objection to the processing in an appropriate case.[627]

---

621 DP Act of 1998 s 22(2).

622 DP Act of 1998 s 22(3). The Commissioner may extend this period by fourteen days in special circumstances (DP Act of 1998 s 22(4)).

623 DP Act of 1998 s 22(5).

624 DP Act of 1998 s 22(6). This is a strict liability offence since no defence is provided. All the offences relating to the notification requirement are triable either in the Magistrates' court or the Crown court. On conviction an offender is liable to a maximum fine of £5,000 in the Magistrates' court or an unlimited fine in the Crown court (see DPR *Data Protection Act 1998* 43).

625 Lloyd *Data Protection Act 1998* 35.

626 Jay & Hamilton *Data protection* 147.

627 Jay & Hamilton *Data protection* 147.

4.3.8 Enforcement of Act by Commissioner

Part V of the DP Act of 1998 deals with methods by which the Commissioner can seek to ensure compliance with the Act by data controllers.[628] These methods involve the serving of notices, namely information notices and enforcement notices, and the making of an assessment, after receiving a request to do so, as to whether the processing of specific personal data complies with the Act.[629]

4.3.8.1 Request for assessment

As stated previously, any person who believes himself or herself to be directly affected by any processing of personal data may ask the Commissioner to assess whether or not it is likely that the processing has been or is being carried out in compliance with the Act.[630] Depending on the Commissioner's assessment, this may lead to enforcement action being taken by the Commissioner pursuant to the complaint.[631]

4.3.8.2 Information notice

a General

The DP Act enables the Commissioner to serve a notice, known as an information notice, on a data controller requiring the data controller to furnish information.[632] The purpose of the notice is to allow the Commissioner to gather sufficient information to determine whether the data controller is processing

628 See Chalton et al *Encyclopedia of data protection* par 1–146/1.

629 Also see par 4.3.5.7.

630 DP Act of 1998 s 42(1). See par 4.3.5.7.

631 See also par 4.3.8.1.

632 DP Act of 1998 s 43. Chalton et al *Encyclopedia of data protection* par 1–146/3 point out that an information notice may only be served on data controllers – not on data processors. Except in respect of data controllers, the Commissioner is therefore powerless to obtain information, including information as to whether a person is a data controller.

in contravention of the statutory provisions.[633]

The Commissioner may serve an information notice in one of two situations:

- after receiving a request to make an assessment[634]

- on his or her own initiative where the Commissioner reasonably requires information to determine whether the data controller has complied with or is complying with the data protection principles

The notice must specify the time within which the data controller should respond, as well as the form the response should take.[635] If the Commissioner has served the notice following an application for an assessment, the notice must contain a statement indicating this. In other cases the information notice must indicate that the Commissioner regards the specified information as relevant for the purpose of determining whether the data controller is complying with the data protection principles and the reasons for why the Commissioner regards the information as relevant for that purpose.[636]

There is a right of appeal to the Data Protection Tribunal against an information notice,[637] and the notice must contain particulars of this right.[638] If an appeal is in fact brought, the information need not be furnished before either determination or withdrawal of the appeal. There is a provision for urgency, so

633 Carey *Data Protection Act 1998* 65. Under the DP Act of 1984 the Registrar was unable to compel data users to give answers to questions and this restricted the Registrar's ability to enforce the Act (see Chalton et al *Encyclopedia of data protection* par 1–146/2).

634 See par 4.3.8.1.

635 DP Act of 1998 s 43(1).

636 DP Act of 1998 s 43(2). Chalton et al *Encyclopedia of data protection* par 1–146/4 point out that a notice served pursuant to a third party's request for assessment may address any issue relating to compliance with the provisions of the Act; by contrast a notice served for purposes of determining compliance with the data protection principles is restricted to information relating to such compliance.

637 DP Act of 1998 s 48.

638 DP Act of 1998 s 43(3).

that information may be required to be furnished after seven days, beginning with the day on which the notice is served, without deferral pending an appeal.[639]

The Commissioner may cancel an information notice by written notice to the person on whom it was served,[640] but may not vary the terms of the notice.[641]

It is an offence to fail to respond to an information notice,[642] but it is a defence for a person charged with such an offence that he or she exercised all due diligence to comply with the notice.[643] It is also an offence to knowingly or recklessly make a false statement in purported compliance with the notice.[644]

b Exemptions

Legal professional privilege and the privilege against self-incrimination are protected by exemptions to the duty to comply with an information notice.[645] A person may refuse to comply with an information notice where compliance would reveal one or more of the following:

- the content of any communication between a professional legal adviser and his or her client in connection with the giving of legal advice to the client with respect to his or her obligations, liabilities or rights under this Act[646]

639 DP Act of 1998 s 43(5).

640 DP Act of 1998 s 43(9).

641 Jay & Hamilton *Data protection* 310.

642 DP Act of 1998 s 47(1).

643 DP Act of 1998 s 47(3).

644 DP Act of 1998 s 47(2).

645 Chalton et al *Encyclopedia of data protection* par 1–146/4.

646 DP Act of 1998 s 43(6)(a).

- the content of any communication between a professional legal adviser and his or her client, or between such an adviser or his or her client and another person, made in connection with or in contemplation of proceedings under the DP Act (including proceedings before the Tribunal) and for the purposes of such proceedings[647]

- evidence of the commission of an offence other than an offence under the DP Act, that will expose that person to proceedings for the offence[648]

c Information notice in the case of special purposes

The Commissioner may not serve a standard information notice on a data controller with respect to the processing of personal data for the special purposes (journalism, literature and art)[649] unless he or she has made a determination under section 45(1) that personal data are not being processed only for the special purposes, or are not being processed with a view to the publication by a person of journalistic, literary or artistic material which has not previously been published by the data controller.[650] Where such determination has been made, the data controller must be notified of the determination and the notice must contain particulars of the right of appeal to the Tribunal.[651]

The Commissioner may serve a special information notice on the data controller, but only if one of two conditions apply:[652]

647 DP Act of 1998 s 43(6)(b).

648 DP Act of 1998 s 43(8).

649 See par 4.3.6.2.a.

650 Also see text to fn 518.

651 Conferred by DP Act of 1998 s 48.

652 DP Act of 1998 s 44(1).

- the Commissioner has received a request for assessment[653]

- the Commissioner has reasonable grounds for suspecting that, in a case in which proceedings have been stayed under section 32,[654] the personal data to which the proceedings relate are not being processed only for the special purposes, or are not being processed with a view to the publication by a person of journalistic, literary or artistic material which has not previously been published by the data controller

The special information notice requires of the data controller to furnish the Commissioner, within a specified time and in a specified form, with information for the purpose of ascertaining whether the personal data are being processed only for the special purposes, or whether they are being processed with a view to the publication by a person of journalistic, literary or artistic material which has not previously been published by the data controller.[655]

The special information notice must, like the standard notice, contain the ground on which the notice is served,[656] particulars of the right of appeal,[657] and the period of time allowed for a response. There are also urgency provisions similar to those applicable to the information notices,[658] and the same grounds on which a person may refuse to comply with an ordinary information notice are also available in the case of a special information notice.[659] The Commissioner may also cancel a special information

653 See par 4.3.8.1.

654 See text to fn 516 .

655 DP Act of 1998 s 44(2).

656 DP Act of 1998 s 44(3).

657 DP Act of 1998 s 44(4).

658 On the time period allowed, see DP Act of 1998 ss 44(5) and(6).

659 DP Act of 1998 s 44(7).

notice.[660] Failure to respond to a special information notice is an offence,[661] but it is a defence for a person charged with such an offence that he or she exercised all due diligence to comply with the notice.[662] It is also an offence to knowingly or recklessly make a false statement in purported compliance with the notice.[663]

4.3.8.3 Enforcement notice

a General

The Commissioner may serve an enforcement notice on a data controller if he or she is satisfied[664] that the data controller has contravened or is contravening any of the data protection principles. The purpose of such a notice is to compel the data controller to comply with the principle or principles in question, by requiring the data controller to take, or refrain from taking, specified steps or to refrain from processing personal data (or personal data of a specified description) altogether, or from processing for a specified purpose or in a specified manner.[665] A factor to consider in deciding whether to serve an enforcement notice is whether the contravention has caused or is likely to cause any person damage or distress.[666]

An enforcement notice in respect of a contravention of the fourth data protection principle (which requires the data controller to rectify, block, erase or destroy inaccurate data) may also require the data

660 DP Act of 1998 s 44(10).

661 DP Act of 1998 s 47(1).

662 DP Act of 1998 s 47(3).

663 DP Act of 1998 s 47(2).

664 The Commissioner must not merely suspect that a principle has been breached; he or she must be satisfied that this is the case. "'Satisfaction' suggests a higher quality of evidence than would be required by a 'suspicion' test" (Jay & Hamilton *Data protection* 305).

665 DP Act of 1998 s 40(1).

666 DP Act of 1998 s 40(2). It is not essential that damage or distress actually be established (Jay & Hamilton *Data protection* 305).

controller to rectify, block, erase or destroy other data held by him or her and containing an expression of opinion which appears to be based on the inaccurate data.[667] Where in the case of an enforcement notice relating to the fourth data protection principle, the data accurately record information received or obtained by the data controller from the data subject or a third party, the notice may require the data controller either –

- ❒ to rectify, block, erase or destroy inaccurate data and any other data containing an expression of opinion, or

- ❒ to take specified steps to check the accuracy of the data and, if the Commissioner thinks fit, to supplement the data with a statement of the true facts[668]

Where an enforcement notice requires the data controller to rectify, block, erase or destroy personal data, or the Commissioner is satisfied that personal data which have been rectified, blocked, erased or destroyed had been processed in contravention of any of the data protection principles, an enforcement notice may, if reasonably practicable, require the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction. In determining whether it is reasonably practicable to require such notification, the number of persons who would have to be notified is a factor to consider.[669]

An enforcement notice must contain a statement of the data protection principle or principles which are being contravened and must advance reasons for this statement, as well as give particulars of the rights of appeal conferred by section 48.[670] It must also contain particulars of the time allowed for

667 DP Act of 1998 s 40(3). This is a new power which did not exist under the DP Act of 1984. See Chalton et al *Encyclopedia of data protection* par 1-146/1.

668 DP Act of 1998 s 40(4).

669 DP Act of 1998 s 40(5).

670 DP Act of 1998 s 40(6).

compliance.[671]

Notification regulations yet to be made may make provision as to the effect of the service of an enforcement notice on an entry (relating to the person on whom the notice is served) in the register maintained by the Commissioner.[672]

It is an offence to fail to respond to an enforcement notice,[673] but it is a defence for a person charged with such an offence that he or she exercised all due diligence to comply with the notice.[674] It is also an offence to knowingly or recklessly make a false statement in purported compliance with the notice.[675]

The Commissioner may cancel or vary the notice in writing if he or she considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with the data protection principle or principles to which it relates.[676]

Where there has been a change of circumstances, a person on whom an enforcement notice has been served may, after the expiry of the period allowed for an appeal, apply in writing to the Commissioner for the cancellation or variation of that notice.[677] There is a right to appeal to the Tribunal against the

671 On the time allowed for compliance and provisions regarding urgent matters, see DP Act 998 s 40(7) & (8).

672 DP Act of 1998 s 40(10). Under the DP Act of 1984 the Registrar could have served a data controller with a de-registration notice. This concept is not repeated in the DP Act of 1998, but the notification regulations yet to be announced may ensure continuing control over registration (see Chalton et al *Encyclopedia of data protection* par 1-150/2).

673 DP Act of 1998 s 47(1).

674 DP Act of 1998 s 47(3).

675 DP Act of 1998 s 47(2).

676 DP Act of 1998 s 41(1). This is a new power which did not exist under the DP Act of 1984 (see Chalton et al *Encyclopedia of data protection* par 1-146/1).

677 DP Act of 1998 s 41(2).

refusal of an application for cancellation or variation of the notice.[678]

b Enforcement notice in the case of special purposes

As in the case of information notices, the Commissioner may only serve an enforcement notice on a data controller with respect to the processing of personal data for the special purposes (journalism, literature and art) in specified circumstances.[679] An enforcement notice may only be served if the Commissioner has made a determination under section 45(1)[680] which has taken effect,[681] and the court has granted leave for the notice to be served.[682] The court will not grant such leave unless it is satisfied of two things:

- that the Commissioner has reason to suspect a contravention of the data protection principles which is of substantial public importance

- that the data controller has been given notice, in accordance with the rules of court, of the application for leave (except where the case is one of urgency)[683]

In practice enforcement notices are unlikely to be applicable to personal data held solely for journalistic purposes since, subject to certain conditions, such personal data are exempt from all the data protection principles except the seventh, which deals with security.[684]

678 DP Act of 1998 s 48(2).

679 See par 4.3.8.2.c.

680 Ie that personal data are not being processed only for the special purposes or are not being processed with a view to the publication by a person of journalistic, literary or artistic material which has not previously been published by the data controller. Also see text to fn 518.

681 DP Act of 1998 s 46(3).

682 DP Act of 1998 s 46(1).

683 DP Act of 1998 s 46(2).

684 See Chalton et al *Encyclopedia of data protection* par 1-146/1 and see par 4.3.6.2.e.

4.3.8.4 Rights of appeal

As was noted previously, the following persons have a right to appeal to the Tribunal:[685]

- a person on whom an enforcement notice, an information notice or a special information notice has been served[686]
- a person whose application for cancellation or variation of an enforcement notice has been refused[687]
- a data controller in respect of whom a determination has been made under section 45[688]

There is a right of appeal against the decision of the Tribunal on a point of law to the appropriate court.[689]

685 The appeal proceedings are worked out in more detail in schedule 6 to the Act (see DP Act of 1998 s 48(5)), and schedule 9 on powers of entry and inspection also has effect (see DP Act of 1998 s 50). On the Tribunal, see par 4.3.9.2, 4.3.10.2.

686 DP Act of 1998 s 48(1). If the Tribunal considers that the notice against which the appeal is brought is not in accordance with the law, or to the extent that the notice involved an exercise of discretion by the Commissioner, that the discretion ought to have been exercised differently, the Tribunal must allow the appeal or substitute such other notice or decision as could have been served or made by the Commissioner; and in any other case the Tribunal must dismiss the appeal (see DP Act of 1998 s 49(1)). On such an appeal, the Tribunal may review any determination of fact on which the notice in question was based (DP Act of 1998 s 49(2)).

687 DP Act of 1998 s 48(2). If the Tribunal considers that the enforcement notice ought to be cancelled or varied by reason of a change in circumstances, the Tribunal must cancel or vary the notice (DP Act of 1998 s 49(3)).

688 DP Act of 1998 s 48(4). On DP Act of 1998 s 45, also see text to fn 518. On an appeal under s 48(4), the Tribunal may cancel the determination of the Commissioner (DP Act of 1998 s 49(5)).

689 DP Act of 1998 s 49(6). The appropriate court in England or Wales is the High Court of Justice, in Scotland the Court of Session, and in Northern Ireland the High Court of Justice.

4.3.9 Data Protection Commissioner and Tribunal

The Directive requires that member states should establish one or more independent public authorities to monitor the application of the data protection provisions adopted pursuant to the Directive.[690] The DP Act of 1998 establishes the office of Data Protection Commissioner and a Tribunal.[691]

4.3.9.1 Data Protection Commissioner[692]

a Appointment, status, tenure of office, salary, officers[693]

The office originally established by the Data Protection Act of 1984 as the office of Data Protection Registrar continues to exist but is now known as the office of Data Protection Commissioner.[694] The Data Protection Commissioner is an independent officer who is appointed by Her Majesty the Queen and who reports directly to Parliament.[695]

The Commissioner holds office for five years, and may be relieved of his or her office by Her Majesty at the Commissioner's own request. The Commissioner may also be removed from office by Her Majesty in pursuance of an Address from both Houses of Parliament. If not removed from office, the

690 Dir 95/46/EC art 28(1).

691 DP Act of 1998 s 6.

692 Since 2001 the Data Protection Commissioner is known as the Information Commissioner. This new post was created to combine enforcement of the Data Protection Act of 1998 and the Freedom of Information Act of 2000, which was passed on 30 November 2000 and must be fully in force by 30 November 2005. The Freedom of Information Act gives a general right of access to all types of recorded information held by public authorities. The Information Commissioner is responsible for the implementation of the Freedom of Information Act. This involves promoting good practice; approving and assisting in the preparation of publication schemes; providing information as to the public's rights under the Act; and enforcing compliance with the Act. See also the general introduction to the Act on the Commissioner's website (http://www.dataprotection.gov.uk/).

693 The administrative details pertaining to the office of the Data Protection Commissioner are worked out in sch 5 part 1 of the DP Act. This paragraph is only a brief summary of the details of the Act.

694 DP Act of 1998 s 6(1).

695 DP Act of 1998 s 6(2); sch 5 par 1(2); DPR *Data Protection Act 1998* 37.

Commissioner vacates the office at the age of sixty-five years, or on completing his or her fifteenth year of service, whichever date is the earlier. The Commissioner may only be appointed for more than two terms if his or her reappointment is desirable in the public interest.[696] The Commissioner receives a salary (and a pension) determined by the House of Commons.[697]

The Commissioner must appoint a deputy commissioner, and may also appoint such number of other officers and staff as he or she may determine. The remuneration and other conditions of service of the persons appointed are determined by the Commissioner, subject to the approval of the Secretary of State.[698]

The deputy commissioner must perform the functions of the Commissioner during any vacancy in that office or at any time when the Commissioner is for any reason unable to act. The Commissioner may delegate his or her functions to the staff members.[699]

The Secretary of State may make payments to the Commissioner out of money provided by Parliament.[700] All fees received by the Commissioner in the exercise of his or her functions must be paid to the Secretary of State.[701] It is the duty of the Commissioner to keep proper accounts and to prepare financial statements. These statements are subject to examination by the Comptroller and Auditor-General.[702]

696 DP Act of 1998 sch 5 par 2.

697 DP Act of 1998 sch 5 par 3.

698 DP Act of 1998 sch 5 par 4.

699 DP Act of 1998 sch 5 par 5.

700 DP Act of 1998 sch 5 par 8.

701 DP Act of 1998 sch 5 par 9.

702 DP Act of 1998 sch 5 par 10.

b Functions and duties

The general duties of the Commissioner include:[703]

- promotion of the following of good practice[704] by data controllers and of the observance of the requirements of the Act by data controllers[705]
- arranging for dissemination of information to the public about the operations of the Act, about good practice, and about other matters within the scope of the Commissioner's functions under the Act, and giving advice to any person on those matters[706]
- where the Secretary of State so directs or the Commissioner considers it appropriate to do so, after consultation with trade associations, data subjects or persons representing data subjects, the preparation and dissemination of codes of practice for guidance as to good practice[707]
- encouraging trade associations to prepare and disseminate codes of practice, and where trade associations submit codes of practice, considering the code, and after consultation with data subjects or persons representing data subjects, notifying trade associations as to whether in the Commissioner's opinion the code promotes the following of good practice[708]
- arranging for the dissemination of Community findings or decisions of the European Commission, and of other information that would appear to be expedient to give to data controllers about the protection of the rights and freedoms of data subjects in countries and

703 The Commissioner may, with the consent of the Secretary of State, charge for services provided (DP Act of 1998 s 51(8)).

704 The DP Act of 1998 s 51(9) defines "good practice" as such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, and includes (but is not limited to) compliance with the requirements of the Act.

705 DP Act of 1998 s 51(1).

706 DP Act of 1998 s 51(2).

707 DP Act of 1998 ss 51(3).

708 DP Act of 1998 s 51(4).

territories outside the EEA[709]

- ❒ assessing, with the consent of the data controller, any processing of personal data for the following of good practice and informing the data controller of the results of the assessment[710]
- ❒ annually laying before each House of Parliament a general report on the exercise of his or her functions under the Act[711]
- ❒ laying before each House of Parliament any code of practice prepared as directed by the Secretary of State[712]
- ❒ assisting individuals, on application, who are parties to proceedings which relate to personal data processed for the special purposes[713]
- ❒ being the designated authority for international cooperation as required by the Convention and the Directive[714]

Other functions or duties of the Commissioner which have already been discussed include:

- ❒ maintaining a register of persons who have given notification[715]
- ❒ making a preliminary assessment of data processing activities[716]
- ❒ making an assessment, at the request of a person, as to whether or not it is likely that any

709 DP Act of 1998 s 51(6).

710 DP Act of 1998 s 51(7).

711 DP Act of 1998 s 52.

712 DP Act of 1998 ss 51(3) and 52(3).

713 DP Act of 1998 s 53. The Commissioner must only grant such an application if in his or her opinion the case involves a matter of substantial public interest (DP Act of 1998 s 53(2)). Such assistance may include the Commissionerbearing the costs of legal advice, including representation arising from any proceedings (see also DP Act of 1998 sch 10 and Chalton et al *Encyclopedia of data protection* par 1–355/3).

714 DP Act of 1998 s 54.

715 See par 4.3.7.6.

716 See par 4.3.7.7.

processing of personal data has been or is being carried out in compliance with the Act[717]

- submitting to the Secretary of State proposals as to the provisions to be included in the first notification regulations[718]

c Obligation of confidentiality

The Commissioner and his or her staff may be guilty of an offence where they knowingly or recklessly disclose information that relates to an identified or identifiable individual or business, that has been obtained by the Commissioner for the purposes of the DP Act of 1998, and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority.[719]

d Powers of entry, inspection and seizure

We have already discussed the Commissioner's power to serve information and enforcement notices and to make an assessment in order to enforce the provisions of the DP Act.[720]

The Act also grants the Commissioner a power of entry and inspection in order to perform his or her duties under the Act. This power is subject to the issue of a warrant by a circuit judge.[721] The judge may issue a warrant if he or she is satisfied on the basis of information supplied by the Commissioner on oath that there are reasonable grounds for suspecting that a data controller is contravening any of the data protection principles, or that an offence under this Act is being committed, and that evidence

717 See par 4.3.8.1

718 See fn 574. The Commissioner must also keep under review the working of the notification regulations and fromtime to time submit to the Secretary of State proposals as to amendments to be made to the regulations (DP Act of 1998 s 25(2)).

719 DP Act of 1998 ss 59(1) and (3). See also par 4.3.10.2.

720 See par 4.3.8.

721 The Directive requires member states to grant national supervisory authorities investigative powers, including powers of access to data forming the subject matter of processing activities (Dir 95/46/EC a 28(3)). However, the government has decided against granting the Commissioner any independent right to enter and investigate premises (see Chalton et al *Encyclopedia of data protection* par 1–355/4).

of the contravention or of the commission of the offence is to be found on any premises specified in the information.[722]

A judge may not issue a warrant in respect of any personal data processed for the special purposes unless a determination by the Commissioner under section 45[723] with respect to those data has taken effect.[724] The warrant must authorise the Commissioner or any of his or her officers or staff at any time within seven days of the date of the warrant to enter the premises, to search them, to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal data and to inspect and seize any documents or other material found there which may be such evidence.[725]

The powers of inspection and seizure conferred by a warrant are not exercisable in respect of:

- personal data which by virtue of section 28 (national security) are exempt from any of the provisions of the Act[726]

- any communication between a professional legal adviser and his or her client in connection with the giving of legal advice to the client with respect to his or her obligations, liabilities or rights under the Act, or such communication made in connection with proceedings under the Act[727]

Any person who intentionally obstructs a person in the execution of a warrant or fails without

722 DP Act of 1998 sch 9 par (1).

723 See fn 518.

724 DP Act of 1998 sch 9 par 1(2).

725 DP Act of 1998 sch 9 par 1(3). For more details on the issuing and execution of the warrants, see DP Act of 1998 sch 9 par 2–7.

726 DP Act of 1998 sch 9 par 8.

727 DP Act of 1998 sch 9 par 9(1). This exception does not apply to anything in the possession of a person other than the professional legal adviser or his or her client or to anything held with the intention of furthering a criminal purpose (DP Act of 1998 sch 9 par 9(3)).

reasonable excuse to give any person executing such a warrant such assistance as may reasonably be required for the execution of the warrant is guilty of an offence.[728]

4.3.9.2 Data Protection Tribunal

a Appointment, tenure of office, salary, officers, expenses[729]

The Data Protection Tribunal established under the DP Act of 1984 will continue to exist under the DP Act of 1998.[730] It will consist of a chairperson appointed by the Lord Chancellor, as well as deputy chairpersons and other members appointed by the Secretary of State.[731]

The members of the Tribunal must, generally speaking, be lawyers with seven years' experience.[732] The members must represent either the interests of data subjects, or the interests of data controllers.[733]

The members hold and vacate office in accordance with the terms of their appointment. They may be re-elected. They may resign, and the chairperson and deputy chairperson must do so at the age of 70. The Secretary of State decides what remuneration or allowances are paid to members of the Tribunal. The Secretary of State may provide the Tribunal with such officers and staff as he or she thinks necessary for the proper discharge of its functions. The expenses of the Tribunal are defrayed by the Secretary of State out of money provided by Parliament.

728 DP Act of 1998 sch 9 par 12.

729 DP Act of 1998 sch 5 part 2 para 12 – 15.

730 DP Act of 1998 s 6(3).

731 DP Act of 1998 s 6(4).

732 DP Act of 1998 s 6(5). More precisely, they should be (a) persons who have a 7-year general qualification, within the meaning of section 71 of the Courts and Legal Services Act of 1990, (b) advocates or solicitors in Scotland of at least 7 years' standing, or (c) members of the Bar of Northern Ireland or solicitors of the Supreme Court of Northern Ireland of at least 7 years' standing.

733 DP Act of 1998 s 6(6).

b Functions: hearing of appeals

The function of the Tribunal is to hear appeals. The circumstances under which an appeal may be brought in connection with information- and enforcement notices issued by the Commissioner, and the powers of the Tribunal in that regard, have already been discussed.[734] We have also referred to the fact that a person directly affected by the issuing of a certificate by a Minister exempting personal data from any provisions of the DP Act for the purpose of safeguarding national security may also appeal to the Tribunal against the certificate.[735] The Tribunal may allow the appeal and squash the certificate if it finds that the Minister did not have reasonable grounds for issuing the certificate.[736]

There is a right of appeal against a decision of the Tribunal on a point of law to the appropriate court.[737]

4.3.10 Remedies and sanctions

In terms of the Directive individuals are entitled to administrative and judicial remedies, including receiving compensation from the controller for damage suffered as a result of an unlawful processing operation. The national data protection legislation is also required to lay down the sanctions to be imposed in the event of any infringement of its provisions.[738]

734 See par 4.3.8.4.

735 DP Act of 1998 s 28(4). See par 4.3.6.2.a.

736 DP Act of 1998 s 28(5). See DP Act of 1998 sch 6 for more detail on the appeal proceedings.

737 DP Act of 1990 s 49(6).

738 Dir 95/46/EC a 23 and a 24.

4.3.10.1 Remedies[739]

Under the DP Act of 1989 a court may make an order to enforce the rights of an individual in regard to subject access,[740] the prevention of processing that is likely to cause damage or distress,[741] prevention of direct marketing[742] and the prevention of automatic processing.[743] It may also order a controller to rectify, erase or block incorrect data[744] and make an order to provide for compensation.[745]

An individual may further ask the Commissioner for an assessment of any processing by which he or she believes himself or herself to be directly affected,[746] and may ask for the assistance of the Commissioner in cases involving the special purposes.[747]

4.3.10.2 Criminal offences

a Introduction

The DP Act of 1998 creates a number of offences, some of which have already been referred to, and some of which will now be dealt with. The offences that have been referred to include:

739 The civil and administrative remedies provided for by the Act have already been discussed in previous paragraphs, and will merely be briefly indicated here.

740 See par 4.3.5.1.e.

741 See par 4.3.5.2.c.

742 See par 4.3.5.3.b.

743 See par 4.3.5.4.b.

744 See par 4.3.5.6.

745 See par 4.3.5.5.

746 See par 4.3.8.1.

747 See par 4.3.5.7. Apart from these administrative remedies given to a individual, the Commissioner may of course also enforce the provisions of the Act on his or her own (see par 4.3.8).

- ❒ processing personal data without notification to the Commissioner[748]
- ❒ failure to notify the Commissioner of changes in registrable particulars in the notification register entry[749]
- ❒ commencing assessable processing before expiry of the time allowed for preliminary assessment by the Commissioner of the assessable processing[750]
- ❒ failure to make information available within 21 days and free of charge in response to a request for unnotified particulars[751]
- ❒ failure to comply with an enforcement notice[752]
- ❒ failure to comply with an information notice or a special information notice[753]
- ❒ knowingly or recklessly making a materially false statement in response to an information notice or a special information notice[754]
- ❒ intentional obstruction of, or failure without reasonable excuse to give reasonable assistance to, a person executing a warrant of entry and inspection[755]

b Unlawful obtaining of personal data[756]

It is an offence for a person, without the consent of the data controller, knowingly or recklessly, to obtain or disclose personal data or the information contained in personal data, or procure the disclosure

748 DP Act of 1998 ss 17(1) and 21(1). See par 4.3.7 and fn 579.

749 DP Act of 1998 s 20. See par 4.3.7.2.

750 DP Act of 1998 s 22(6). See par 4.3.7.7 and fn 624.

751 DP Act of 1998 s 24(4). See par 4.3.7.5.

752 DP Act of 1998 ss 40 and 47(1). See par 4.3.8.3 and text to fn 674.

753 DP Act of 1998 ss 43, 44 and 47(1). See par 4.3.8.2.

754 DP Act of 1998 s 47(2). See par 4.3.8.2.

755 DP Act of 1998 sch 9 par 12. See par 4.3.9.1.

756 See also Jay & Hamilton *Data protection* 322–323; Bainbridge *Data protection law* 152–153.

to another person of the information contained in personal data.[757]

The Act provides specific exceptions to liability for this offence where the person can show one of the following:

- that the obtaining, disclosing or procuring was necessary to prevent or detect crime, or was required or authorised by law
- that he or she acted in the reasonable belief that he or she had the legal right to obtain, disclose or procure the disclosure
- that he or she acted in the reasonable belief that the data controller would have consented to the obtaining, disclosing or procuring if the data controller had known
- that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest[758]

"Personal data" does not include data which are exempt from this section of the Act by virtue of the national security exemption.[759]

c Unlawful selling of personal data

If a person has obtained personal data unlawfully, it is an offence to sell or offer to sell such data. An advertisement indicating that personal data are or may be for sale is an offer to sell the data.[760]

757 DP Act of 1998 ss 55(1) and 55(3).

758 DP Act of 1998 s 55(2).

759 DP Act of 1998 s 55(8) and see par 4.3.6.2.

760 DP Act of 1998 ss 55(4) and (5). See also Bainbridge *Data protection law* 152–153.

"Personal data" includes information extracted from personal data for the purposes of these offences.[761] Personal data do not include data which are exempt from this section of the Act by virtue of the national security exemption.[762]

d Enforced subject access[763]

It is an offence for persons to require another person or a third party to supply them with a "relevant record"[764] or to produce a relevant record to them in either of the following two situations:

- in connection with the recruitment of that other person as an employee, the continued employment of that other person, or any contract for the provision of services to them by that other person

- where a person is concerned with providing (for payment or not) goods, facilities or services to the public or a section of the public, as a condition of providing or offering to provide any goods, facilities or services to that other person[765]

The Act provides statutory exceptions to liability for this offence where the person can show one of the following:

- that the imposition of the requirement was required or authorised by law

761 DP Act of 1998 s 55(7).

762 DP Act of 1998 s 55(8) and see par 4.3.6.2.

763 See also Jay & Hamilton *Data protection* 324; Bainbridge *Data protection law* 153–154.

764 The term "relevant record" is defined in the Act by reference to a schedule which lists data controllers and the subject matter of subject access requests that may be made to them by data subjects. Generally, the term relates to records of cautions, criminal convictions and to certain social security records relating to the data subject (see DP Act of 1998 s 56(6)).

765 DP Act of 1998 ss 56(1), (2) and (5).

- that in the particular circumstances the imposition of the requirement was justified as being in the public interest[766]

The Act specifically provides that the imposition of the requirement is not to be regarded as being justified as being in the public interest on the grounds that it would assist in the prevention or detection of crime.[767] This is because of the provisions of part V of the Police Act of 1997 which provide for the issuing of certificates of criminal records among other things.[768]

If persons charged with this offence are unable to show that they satisfy one of the exceptions, the offence is one of strict liability.[769]

e *Unlawful disclosure of information by Commissioner or staff*

It is an offence for the Commissioner, a member of the Commissioner's staff or an agent of the Commissioner, past or present, to knowingly or recklessly disclose, without lawful authority, information which

- has been obtained by, or provided to, the Commissioner under or for the purposes of the Act
- relates to an identified or identifiable individual or business
- is not at the time of the disclosure, and has not previously been, available to the public from other sources

766 DP Act of 1998 s 56(3).

767 DP Act of 1998 s 56(4).

768 DP Act of 1998 s 56(4). These offences may not be brought into effect until the provisions of the Police Act of 1997 in relation to criminal conviction certificates are in force (DP Act of 1998 s 75(4)). See also Chalton et al *Encyclopedia of data protection* par 1–060/16; Uglow 1998 *Crim L R* 235–245.

769 DPR *Data Protection Act 1998* 45.

A disclosure of information is made with lawful authority only if:

- the disclosure is made with the consent of the individual or of the person who is carrying on the business for the time being
- the information was provided for the purpose of its being made available to the public under any provision of the Act
- the disclosure is made for the purposes of, and is necessary for, the discharge of any functions under the DP Act or any Community obligation
- the disclosure is made for the purposes of any proceedings (whether criminal or civil and whether arising under the DP Act or otherwise)
- having regard to the rights and freedoms or legitimate interests of any person, the disclosure is necessary in the public interest[770]

This provision is likely to restrict the ability of the Commissioner's office to use the threat of bad publicity as an enforcement mechanism against data controllers.[771]

f General provisions relating to offences

All the above offences (except the intentional obstruction of, or failure without reasonable excuse to give

770 DP Act of 1998 s 59(2).

771 See Chalton et al *Encyclopedia of data protection* par 1–355/4. The then Registrar, Mrs France, objected to the potential ease with which the activities of her staff could be criminalised and called for the provision in the Bill to be removed or amended to include an element of potential damage (see DPR *Criminal disclosures*). The government, on the other hand, stated that the provision was required to comply with a 28(7) of the Directive, which requires the members and staff of the supervisory authority, even after their employment ended, to be subject to a duty of professional secrecy (see Chalton et al *Encyclopedia of data protection* par 1–355/4).

reasonable assistance to, a person executing a warrant of entry and inspection[772]) are triable in either the Magistrates' court or the Crown court. Upon conviction in the Magistrates' court, an offender is liable to a maximum fine of £5,000 but in the Crown court an unlimited fine may be imposed.[773]

The Act provides for separate personal liability for any of the offences in the Act for directors or other officers of any company which has committed an offence under the Act. Where it is proved that the company committed the offence with the consent or connivance of, or due to any neglect on the part of, the officer concerned, that person will be guilty of the offence jointly with the company and will be liable to be proceeded against and punished accordingly. The same applies to members of a company in respect of those companies which are managed by their members, as well as, in Scotland, a partner of a Scottish partnership.[774]

5 SUMMARY

In brief, the position in the UK is as follows: English common law does not recognise the right to privacy. Constitutional protection of the right to privacy is provided by the Human Rights Act of 1998, which guarantees that individuals have the right to respect for their private and family lives, their homes and correspondence. However, the protection of the right to privacy provided by this Act is not significant from a data protection point of view. In the UK, data protection is essentially provided through legislation, and in particular through the Data Protection Act of 1998 which replaces the first Data Protection Act of 1984. The 1998 Act implements the provisions of the EU Directive on data protection although in some aspects it seems to be more restrictive than the Directive. Since the Act implements the provisions of the Directive, the general principles are very good. However, the Act is

772 Ie DP Act of 1998 sch 9 par 12.

773 DP Act 1998 s 60(2) and (3); DPR *Data Protection Act 1998* 45–55. In England or Wales proceedings for a criminal offence under the Act can be commenced only by the Commissioner or by (or with) the consent of the Director of Public Prosecutions. In Scotland, criminal proceedings will normally be brought by the Procurator Fiscal. In Northern Ireland, proceedings for an offence under the Act can be commenced only by the Commissioner or by (or with) the consent of the Director of Public Prosecutions for Northern Ireland (DP Act of 1998 s 60(1)).

774 DP Act of 1998 s 61.

very complicated and involved, and therefore, it is suggested, does not represent an ideal model for South Africa to follow.