Chapter 27

# The UK's Implementation of Directive 95/46/EC

Deryck Beyleveld*, Andrew Grubb†, David Townend‡, Ryan Morgan** and Jessica Wright††

## Introduction: The Data Protection Act

The UK has implemented Directive 95/46/EC via the Data Protection Act 1998, which received Royal Assent in June 1998, and was brought into force on 1 March 2000. Subsequently, minor modifications to the Act have been introduced by the Freedom of Information Act 2000. These include new duties for the Information Commissioner (for example, enforcement of the Act), a new name, a general right of access to all types of 'recorded' information held by public authorities and those providing services for them (and details exemptions), and it also places obligations on public authorities to, for example, inform the public about the kinds of information that authority publishes.

The Data Protection Act itself has six parts. Part I (ss.1–6) provides definitions of, for example, personal data, data controller, data subject, data processor, processing, sensitive personal data, specifies where the Act applies and makes provision for the Supervisory Authority (originally the Data Protection Commissioner, but now the Information Commissioner) and the Information Tribunal (originally the Data Protection Tribunal). Part II (ss.7–15) provides data subjects with rights to access, to prevent processing likely to cause damage or distress, to prevent processing for purposes of direct marketing, in relation to automated decision-making, to compensation for damages causes by processing, and to obtain rectification, blocking, erasure and destruction of data through a Court. Part III (ss.16–26) specifies the duties of data controllers to notify processing to the Supervisory Authority. Part IV (ss.27–39) provides general exemptions, which include an exemption for research, history and statistics (s.33). Part V (ss.40–50) specifies the powers of enforcement of the Supervisory

---

* Director of the Sheffield Institute of Biotechnological Law and Ethics based at Sheffield University Department of Law and Professor of Jurisprudence.
† Professor of Medical Law at Cardiff Law School.
‡ Sub-Dean (Postgraduate Studies) in the Faculty of Law of the University of Sheffield.
** Research Assistant at Cardiff Law School.
†† PRIVIREAL co-ordinating co-worker based at Sheffield University Department of Law.

Authority and provides for appeals to the Information Tribunal against the exercise of these powers. Part VI (ss.51–75) makes miscellaneous provisions. These include detailing the functions of the Information Commissioner (ss.51–75); making obtaining, disclosure or selling of personal data or of information contained in it (s.55) an offence; providing for prosecutions and penalties under the Act (s.60); defining an 'accessible record' (which includes a 'health record' (s.68)), a 'health professional' (s.69); and providing other 'supplementary definitions' (s.70).

The Act further contains 16 Schedules, the most relevant of which are outlined here. Schedule 1 provides for eight data protection principles, which (see s.4(4)) provide the general duties of the data controller. These are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
   a. at least one of the conditions in Schedule 2 is met, and
   b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area 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 (Schedule 1 Part I).

The first five principles reflect Article 6(1)(a)–(e) of the Directive. The way in which the Act elaborates the 1st data protection principle means that Articles 7 and 8 (implemented in Schedules 2 and 3 of the Act as requirements of lawful processing) and Articles 10 and 11 (implemented in Schedule 1 Part II paragraphs 2 and 3 as requirements of fair processing) are viewed as elaborating the 1st principle.

The 6th principle reflects a duty to comply with the rights granted by the Act in Sections 7, 10, 11 and 12, as specified by Schedule 1 Part 2 paragraph 8.

The 7th principle relates to Article 17 of the Directive (Security of Processing), and is specified in Schedule 1 Part II paragraph 9.

The 8th principle relates to Articles 25 and 26 (Transfer of data to third countries) of the Directive and is specified in Schedule 1 Part II paragraph 13 and Schedule 4.

Schedules 2 and 3, which are conditions of lawful processing under the 1st data protection principle, implement Articles 7 and 8.

Schedule 8 provides transitional exemptions up until 23 October 2007.

Schedule 13 lists modifications to the Act that apply before 23 October 2007 in relation to manual data that are exempt during that period.

The Act itself is supplemented by numerous statutory instruments that have been passed under the Act (22 at the time of writing), the most important of which for the purposes of medical research is The Data Protection (Processing of Sensitive Personal Data) Order 2000, No. 417.

## Confidentiality and Common Law

Confidentiality, as a legal duty, has an uncertain basis in common law.[1] One could severally or jointly found an obligation of confidence within contract law, the tort of negligence or equity. In the medical context, health care professionals have long recognized an ethical obligation to maintain confidences in order to encourage patient participation and trust.[2] To the extent that this translates into a legal duty, the Courts have preferred to establish a medical practitioner's duty to maintain patient confidence's as an equitable obligation deriving from the public interest rather than a private duty toward the patient.

### *When is Information Confidential?*

Information is confidential when it is of a confidential nature. This rather circular definition may be derived from a number of cases outside the medical sphere.[3] The common law has further recognized that a confidential relationship of this sort exists between doctor and patient.[4] However, not all forms of information imparted in these circumstances, even where the confidant knows that the information is being provided in confidence, can be classified as confidential, for example, the information might already be public knowledge.[5] This does not mean, of course, that merely because persons other than the confidant know of the confidential information, it may be classified as 'public knowledge'. Those other persons may equally be under an obligation of confidence. Furthermore, information which is adequately anonymized cannot be regarded as confidential information.[6]

---

[1] See, e.g. R. Wacks, 'Breach of Confidence and the Protection of Privacy' (1977) 127 *NLJ* 328, and J. Montgomery, *Health Care Law* (2nd Ed., London: Oxford University Press, 2002), 254–258.

[2] For example, the Hippocratic Oath stipulates 'Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart there from, which ought not to be noised abroad, I will keep silence thereon, counting such things to be as sacred secrets.'

[3] For example, *Coco* v *AN Clark (Engineering) Ltd* [1969] RPC 41.

[4] For example, *Hunter* v *Mann* [1974] QB 767.

[5] See *Saltman Engineering Co.* v *Campbell Engineering Co. Ltd* [1948] 65 RPC 203.

[6] *R v Department of Health, ex parte Source Informatics Ltd* [2000] 1 All ER 786.

*Confidentiality as a Human Right*

Following the Human Rights Act 1998, a duty of confidentiality may now be regarded as an extension of an individual's right to a private life under Article 8 of the European Convention on Human Rights.[7] In *Venables* v *News Group Newspapers Ltd*,[8] for example, the Court recognized that information concerning 'medical, psychological, or therapeutic care is, in principle, confidential'.[9] The deontological basis for this summation, based upon the right to privacy under Article 8, is obvious.

In terms of medical practice, any health care practitioner working under the auspices of the NHS or other state agency must act in a manner compatible with the Convention. This is due to these institutions being 'public authorities' within the meaning of s.6 of the Human Rights Act 1998. This places an obligation on public bodies, or any person who exercises a function which is public in nature,[10] to act in a manner which is consistent with the Convention.

However, processors of medical information who are not employed by bodies whose functions are public in nature do not have a direct duty under the Act. Moreover, medical practitioners, merely by virtue of their registration with the General Medical Council, are not regarded as fulfilling a public function under the jurisprudence of the European Court of Human Rights.[11] An activity essentially of a private character under domestic law, such as the practice of medicine, could not automatically be converted into a public law activity simply because it was subject to administrative authorization and controls by statutorily-based regulatory authorities. However, where the Court is called upon to construe the extent of a duty of confidentiality in any given case, the Court will develop its jurisprudence in line with the Convention.[12] This is because Courts are also 'public authorities' within the meaning of s.6(3)(a) of the Human Rights Act. Consequently, to decide a case in a manner inconsistent with the Convention, or without regard to Strasbourg jurisprudence,[13] would contravene the Act. It is reasonable to assume, therefore, that the Courts will continue to develop the common law surrounding confidentiality in harmony with rights under the Convention. This should be so even where the confidant is entirely within the private sphere.

---

[7] See, e.g. *Douglas* v *Hello! Ltd* [2001] 2 All ER 289 (CA) and *A v B (a company)* [2002] 2 All ER 545 (CA).
[8] [2001] 1 All ER 908.
[9] Ibid. at 939–940.
[10] S. 6(3)(b).
[11] *Konig* v *Federal Republic of Germany* [1980] 2 EHRR 170.
[12] As was accepted in *Venables*, *supra* (n. 8). See also, *A Health Authority v X* [2001] Lloyd's Rep Med 349 (Munby J) and [2002] Lloyd's Rep Med 139 (CA).
[13] An obligation incumbent upon the Court under S. 2(1).

*When may Confidential Information be Lawfully Disclosed?*

Confidentiality has never been regarded as an absolute right under the common law.[14] Firstly, confidential information may be disclosed with the consent of the patient. Secondly, where a patient has not consented, disclosure is permitted where the law either requires or allows it.[15] A recent example is The Health Service (Control of Patient Information) Regulations 2002[16] made pursuant to s.60 of the Health and Social Care Act 2001. In broad terms, these regulations provide for regulated processing of information concerning neoplasia[17] and communicable diseases/public health risks[18] specifically. Also, there is a general provision[19] allowing for processing of confidential patient information for 'medical purposes' set out in the Schedule to the Regulations, subject to registration. Regulation 4 expressly modifies the obligation of confidence so as to resolve any legal conflict.

Finally, confidentiality may be broken where it is in the 'public interest' to do so. To this end, the Court must enter into a 'balancing exercise' weighing the benefits of disclosure against the detriments of breaching confidence.

In what follows, we will answer the questions posed for the project under various subheadings, and in the process of which we will highlight what we consider to be contentious aspects of the UK's implementation.

## Issues in Relation to Data Protection

*The Definition of Personal Data*

Personal data are defined in Section 1(1) as:

> data which relate to a living individual who can be identified—
>
> a. from those data or
> b. from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

---

[14] See, I. Kennedy and A. Grubb *Medical Law* (3rd edn., London: Butterworths, 2000), Chapter 8.

[15] For example, the Road Traffic Act 1988, S. 172(b), where an individual must provide even confidential information to the police regarding certain road traffic offences (see in particular *Hunter v Mann* [1974] 1 QB 767). Other examples include notification procedures under the Abortion Regulations (SI 1991 No. 499) and communication of information for the purposes of preventing the spread of venereal disease (National Health Service (Venereal Diseases) Regulations (SI 1974 No. 29) and NHS Trusts (Venereal Disease) Directions 1991).

[16] SI 2002 No. 1438.

[17] Reg. 2.

[18] Reg. 3.

[19] Reg. 5.

> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

This implies that, where the data subject can be identified only indirectly from the data, the data are personal (and thus fall under the scope of the Act) only if the data controller can identify the data subject indirectly. This is controversial, because the Directive (Article 2(a)) can be read as stating that data remain personal data if *anyone* can identify the data subject from it directly or indirectly. The UK's definition also restricts the scope of the Act to personal data on living individuals. This is controversial as the Directive applies to 'natural persons' (see Article 2(a)) and the customary contrast with 'natural person' is 'legal person' not 'deceased person', a contrast which is reflected in Recital 32 of the Directive. When the patient has died, the personal representatives and anyone with a legal claim arising from the death can obtain access to part or all of the patient's health records (officially only those since 1991) under the Access to Health Records Act 1990 c.23, Section 3.1.

*The Effect of Anonymization*

The act of anonymization is to some extent a controversial issue in UK law, and the prevailing assumption is that the Data Protection Act does not cover the anonymization of data. There is, however, a substantial argument against this assumption. This argument is presented below, and will ultimately have to be resolved in the Courts.

The argument that the act of anonymization will itself be processing of the data, is not without some support from the Information Commissioner:

> [i]n anonymising personal data the data controller will be processing such data and, in respect of such processing, will still need to comply with the provisions of the Act.[20]

Bearing in mind that because processing under the Act includes anything that can be done with personal data, anonymization is itself a process, and since Recital 26 of the Directive specifies that the principle of protection must apply to all personal data, the ruling of the High Court in *Robertson* (made in relation to Section 11 of the Act, which implements Article 14(b) of the Directive) is relevant to this question. *Robertson* ruled that a data controller who envisages data being processed for a purpose by another to whom the controller discloses the data is to be deemed to be processing the data himself or herself for that purpose. Putting these two things together, it would appear that the Act would require the data subject, B, to be informed of processing by A (the data controller) or C (a third party processor) that will occur only after the data obtained by A from B are rendered completely anonymous. Furthermore, at least where data continue to be held by A in personal form, if A releases non-personal information to C that was

---

[20] Information Commissioner, *Data Protection Act 1998: Legal Guidance* (Version 1, Wilmslow: Information Commissioner, 1998), paragraph 2.2.5.

taken from personal data held by A, then A is liable under the Act for any processing of the non-personal information carried out by C.[21]

*Information Contained in Personal Data*

Except for the purposes of Section 55 of the Data Protection Act 1998 (s.55(7)), unless 'the context otherwise requires', obtaining or recording information that is not itself personal data, but which is 'to be contained in' personal data, constitutes obtaining or recording personal data. Similarly, using or disclosing information that is not itself personal data, but which is 'contained in' personal data, constitutes using or disclosing personal data (s.1(2)).

For the purposes of Section 55(4)–(6), '"personal data" includes information extracted from personal data' (s.55(7)).

This suggests that anonymous information that is obtained or recorded in order to include it in personal data and anonymous information that is abstracted from personal data and only then used or disclosed are to be considered personal data (i.e., not to have been rendered anonymous), unless special circumstances relating to the context apply. However, what this context/contexts might be is not explained. The Court of Appeal in *R v Department of Health, ex parte Source Informatics Ltd.*[22] at 799 has expressed the view (*obiter* in our opinion) that the processing of anonymized information (on patient's prescriptions) is not covered by the Directive (and, by implication the Act) except where it 'could impair the patient's own health requirements'. The Court did not, however, refer to Section 1(2) (or Section 55(7)) of the Act in doing so (probably because the Act had not come into force at the time of the judgment). With Section 1(2) in mind, this view is odd because it presumes, contrary to what the wording of the Act suggests, that the use of anonymous information contained in personal data is only to be considered use of personal data in the special case (where anonymization would not be in the patient's interests, e.g., because this precludes it being used for the treatment of the patient, for which it was provided). Although Section 55 does not apply to the facts of the *Source Informatics* case, it is nevertheless relevant to the approach of the Court of Appeal. When Section 55(7) says that Section 1(2) does not apply to Section 55, this means (we suggest) that information contained in personal data is personal data regardless of the context. And, when Section 55(7) says that 'for the purposes of subsections (4) to (6), "personal data" includes information extracted from personal data' this means that, for the purposes of these subsections, information that was abstracted from personal data is personal data even if the data from which it was abstracted no longer exist in personal form (because, if the second clause of Section 55(7) only applies where the source information is still in personal form, the abstracted information could be said to be contained in personal data, and it would not be necessary for Section 55(7) to

---

[21] For a detailed discussion of anonymization, see D. Beyleveld and D. Townend 'When is Personal Data Rendered Anonymous? Interpreting Recital 26 of Directive 95/46/EC' (forthcoming 2004) *Medical Law International*.

[22] *R v Department of Health, ex parte Source Informatics Ltd. supra* n. 6 above.

distinguish the meaning of 'personal data' in Section 55(4)–(6) from its meaning in Section 55 generally).[23]

## Exemptions for Research

### *Compatible and Incompatible Processing*

The UK Act provides a limited exemption for research, history and statistics in Section 33. The further processing of personal data for these purposes is not to be considered incompatible with the purposes for which the data were obtained, provided that 'the relevant conditions' (which are that the data are not processed to support measures or decisions with respect to particular individuals, and the processing is not likely to cause substantial damage or substantial distress to any data subject) are met (s.33(1) and (2)). This is an exemption from what the Act describes as the second part of the 2nd data protection principle (see Schedule 1 Part I; cf. Article 6(1)(b)). No positive definition of 'incompatibility' or 'compatibility' is provided.

### *Adequate Safeguards*

Provided that the relevant conditions are met, Section 33 also exempts processing only for research purposes from the 5th data protection principle (see Schedule 1 Part I; cf. Article 6(1)(e), which requires that personal data are not to be kept for longer than needed for the purposes for which they were originally obtained) (Section 33(3)), and from the duty to provide the data subject with access to the data (see Section 7 of the Act and Article 12(a) of the Directive) where, additionally, the results of the research will not be made available in personal form (Section 33(4)). Since exemption from the Article 6(1)(b) and 6(1)(e) requirements of the Directive is subject to the provision of suitable safeguards and the relevant conditions are the only conditions that need to be satisfied for the exemptions provided from the 2nd and 5th data protection principles, satisfaction of the relevant conditions must be taken to constitute the UK's view of adequate safeguards for these purposes (this also applies to the exemption for research in the substantial

---

[23] The uncertainty caused on this point by the *Source Informatics* judgement (see n. 6 above) remains, despite both an arguably compelling duty on the Court to seek a ruling on the point from the European Court of Justice or on the Department of Health to appeal the decision to the House of Lords. Neither of these courses was taken, the Government instead seeking to reverse the decision quickly through the introduction of a clause into what was to become the Health and Social Care Act 2001, s. 60. The clause would have given the Secretary of State powers, through regulations, to render processing of anonymized data unlawful as well as the processing of confidential patient identifiable data without consent lawful, where this would be in the public interest. The elements in the clause relating to anonymized data, however, were dropped during the passage of the Bill through the House of Lords because of time constraints and political pressure from the Opposition, resulting in a fixing of the Court of Appeal judgement in the law at least for the present time.

public interest created by Statutory Instrument 417, paragraph 9). For the purposes of exemption from Section 7, the UK Act's view of adequate legal safeguards (as required by Article 13(2) for exemption from Article 12 requirements) must be taken to be the relevant conditions plus the requirement not to identify the data subject (as specified in Article 13(2)). Furthermore, on a related issue it must be noted that where data have been anonymized, the Commissioner is of the view that safeguards must be in place to prevent reconstitution of the identifiers:

> It will be incumbent upon anyone processing data to take such technical and organisational measures as are necessary to ensure that the data cannot be reconstituted to become personal data and to be prepared to justify any decision they make with regard to the processing of the data.[24]

In cases other than where personal data are obtained from the data subject, the UK Act exempts from the requirement to provide the data subject with information about the identity of the data controller, etc., if this would require disproportionate effort, the processing is required by a non-contractual legal obligation of the data controller, or any conditions prescribed by the Secretary of State by order are met (Schedule 1 Part 2 paragraph 3). Such derogation, under such conditions (with research purposes explicitly in mind) is made by the Directive subject to appropriate safeguards (see Article 11(2)). However, in this context, the Act makes no specific provision for safeguards.

*Does Preventative Medicine and Medical Diagnosis Cover Medical Research in the UK?*

Schedule 3 paragraph 8(1) follows Article 8(3) in removing a prohibition on the processing of data on a person's health where the processing is for medical purposes and is undertaken by a health professional or one operating under an equivalent duty of confidentiality. However, Schedule 3 paragraph 8(2), unlike the Directive, explicitly includes medical research as a medical purpose.

*When is there no Risk of Breaching Privacy?*

In relation to Article 13(2) of the Directive, which makes research data exempt from the requirement to give access to the data subject on condition, amongst other things, of there being clearly no risk of breaching privacy, it might be tempting to think that the UK law views protection of the data subject's identity as fulfilling this condition. However, non-disclosure of the data subject's identity is an additional explicit requirement of Article 13(2), which implies that the Directive does not consider this to be sufficient. It is possible that the 'relevant condition' of the UK law that contains the requirement that processing be unlikely to cause substantial distress to the data subject fulfils this role (at least in part).

---

[24] Information Commissioner, *Data Protection Act 1998: Legal Guidance* (Version 1, Wilmslow: Information Commissioner, 1998), paragraph 2.2.5.

*Exemptions from the Article 11 Information Provisions*

No explicit exemption by law from the Article 11 requirement to provide data subjects with information about processing in cases where the data are not obtained from the data subject has been made, though Schedule 1 Part II paragraph 3(1) of the UK Act makes provision for such exemption to be made by the Secretary of State by order. However, s.30(1) of the 1998 Act provides that the Secretary of State:

> ...may by order exempt from the subject information provisions, or modify those provisions in relation to, personal data consisting of information as to the physical or mental health or condition of the data subject.

Consequently, the Data Protection (Subject Access Modification) (Health) Order 2000 (SI 2000 No.413) was passed. This provides for restrictions on data subject access to medical records. Furthermore, the Order adds a further exemption to the 'third party identification' rules under s.7(4). Consequently, a data controller is obliged to comply with a subject access request which entails disclosure of information relating to another individual who can be identified from that information, where that other individual falls within the added Section; 7(4)(c). Furthermore, even where a third party who does not fall within the exemptions laid down in s.7(4)(a),(b) and (c) has communicated information to the data controller regarding the data subject, s.7(4) does not operate so as to prevent the data controller from providing any information whatsoever. Quite the reverse. Section 7(5) states:

> In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of information sought by the request; and that subsection is not to be construed as excusing a data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by omission of names or other identifying particulars or otherwise.

*Substantial Public Interest*

Schedule 3 paragraph 10 of the UK Act empowers the Secretary to State to specify circumstances by order under which the prohibition on the processing of personal data of Article 8(1) of the Directive is removed. In relation to this, Article 2 paragraph 9 of Statutory Instrument 2000 No. 417, The Data Protection (Processing of Sensitive Personal Data) Order 2000, specifies that the prohibition is removed where processing is necessary for research purposes that are in substantial public interest on condition that the 'relevant conditions' of Section 33 of the UK Act are satisfied. No explanation is provided of what is in the 'substantial public interest', though the non-binding Explanatory Report to the Order gives archiving as an example.

*Article 13 and Exemptions for Medical Research*

Apart from availing itself of the power granted by Article 13(2) to exempt research from the subject access right in Section 33 of the Act, the UK has not explicitly appealed to Article 13 to make any exemption for medical research. This raises two problems. First, the UK has made no provision in regards to the restriction of subject access in relation to research, to have claims for checks on the lawfulness of processing for research heard by any person as required by Article 28(4). Secondly, the UK has created exemptions for research in the Control of Patient Information Regulations 2002 under Section 60 of the Heath and Social Care Act 2001 that might be interpreted as exemptions from provisions of the Data Protection Act 1998 (and, by implication, modifications of the requirements of the Data Protection Directive as permitted under Article 13).

Section 60(1) of the Health and Social Care Act 2001 gives the Secretary of State the power to make regulations to permit or require the processing of confidential patient information without the patient's consent

> for medical purposes as he/she considers necessary or expedient-
>
> a. in the interests of improving patient care, or
> b. in the public interest

with the consequence that where

> patient information is processed by a person in accordance with the regulations, anything done by him in so processing the information shall be taken to be lawfully done despite any obligation of confidence owed by him in respect of it (s.60(2)(c)).

However, such regulations (which require the approval of both Houses of Parliament) (s64.3) may not make provision

> requiring the processing of confidential patient information for any purpose if it would be reasonably practicable to achieve that purpose otherwise than pursuant to such regulations, having regard to the cost of and the technology available for achieving that purpose (s.60(3))

or

> for requiring the processing of confidential patient information solely or principally for the purpose of determining the care and treatment to be given to particular individuals (s.60(5)). [In relation to which Regulation 1(1)(f) of the Health Service (Control of Patient information) Regulations 2002 (SI 2002 No.1438) is at least questionable.]

According to Section 60(6),

> Without prejudice to the operation of provisions made under subsection (4)(c), regulations under this section may not make provision for or in connection with the

> processing of prescribed patient information in a manner inconsistent with any provision made by or under the Data Protection Act 1998 (c. 29). [The reference here to subsection 4(c) must be intended to be to subsection 2(c), as there is no section 4(c), and section 2(c) states what was stated in clause 4(c) of a draft of the Bill before it was passed.]

The wording here is, at the least, unfortunate, for, read as saying that processing that falls under any regulations passed must be taken to be lawful even if this contravenes the Data Protection Act 1998, Section 60(6) is certainly in contravention of EC law on the assumption that the Act correctly implements Directive 95/46/EC, hence unlawful under the doctrine of the supremacy of EC law. Consequently it must be read as saying no more than that processing that falls under any regulations passed must be taken not to be unlawful *on account of* being in breach of confidentiality.

More specifically, the problem here is that in order to be lawful under the Data Protection Act 1998, processing must not only not breach confidentiality, but must satisfy Schedules 2 and 3 of the Act (cf. Articles 7 and 8) and the fair processing provisions of Schedule 1 Part II paragraphs 2 and 3 (cf. Articles 10 and 11). With this in mind, it might be thought that, *in practice,* regulations passed under the Act will be compatible with the Directive if they satisfy Section 60(3) of the Act, on the grounds that if it is reasonably impracticable to achieve the objectives of the regulations by other means (specifically by obtaining the consent/non-objection of the patient) then it will not be necessary to obtain consent/non-objection. However, in relation to Schedule 2 (cf. Article 7) it must be noted that reasonable impracticability is not stated to be a condition of *permitting* the processing of confidential patient information (only of requiring processing), which also raises questions about the compatibility of the Act with the European Convention on Human Rights, with which the Act was declared to be compatible by the Secretary of State. In relation to the fair processing provisions (Articles 10 and 11), it must be noted that only the Act, not the Directive, makes information provision (which is necessary for there to be any opportunity to object) subject to practicability in the Article 10 case. Furthermore, insofar as the basis of any regulations (see s.60(1)) is that processing is to be permitted/required in the public interest, attention must be drawn to Article 14(a) of the Directive, which requires the right to object to be removed by national legislation if the public interest is to be the basis of legitimate processing under Article 7 (cf. Schedule 2). It is at least questionable that this right can be removed implicitly. Indeed, given the structure of Section 10 of the Data Protection Act 1998, it is arguable that it can only be removed by regulations made under the 1998 Act (specifically under s.(10)(2)(b)), which have not been made). It should be noted also that, although Article 13.1 permits Member States to modify the obligations and rights provided by Articles 6(1), 10, 11(1), 12 and 21 for the rights of others, and medical research arguably protects the rights of others, the Health and Social Care Act does not purport to modify any of these obligations and rights.

Regulation 2 of SI 2002 No.1438 permits confidential patient information 'relating to patients referred for the diagnosis or treatment of neoplasia' to be

processed for medical research approved by research ethics committees that are recognized by a health authority or the Secretary of State (Regulation 1 paragraph (2) & Regulation 2 paragraph (1)(d)); 'subject to'

- the processing being carried out by persons who are (either individually or as members of a class) approved by the Secretary of State and authorized by the person who lawfully holds the information (Regulation 2 paragraphs (1) & (3)),
- the information not being processed more than necessary for the purposes permitted under the Regulations (Regulation 2 paragraph 1 & Regulation 7);
- Regulation 2 paragraph (2), which states

> For the purposes of this regulation, 'processing' includes (in addition to the use, disclosure or obtaining of information) any operations, or set of operations, which are undertaken in order to establish or maintain databases for . . . [*inter alia*, the purpose of medical research approved by research ethics committees] . . ., including –
>
> a. the recording and holding of information;
> b. the retrieval, alignment and combination of information;
> c. the organisation, adaption or alteration of information;
> d. the blocking, erasure and destruction of information;

and

- Regulation 2 paragraph (4), according to which,

> Where the Secretary of State considers that it is necessary in the public interest that confidential patient information is processed for a purpose specified in paragraph (1), he may give notice to any person who is approved and authorized under paragraph (3) to require that person to process that information for that purpose and any such notice may require that the information is processed forthwith or within such period as is specified in the notice.

We find this Regulation difficult to interpret. If the word 'includes' in paragraph (2) has the meaning that it normally has, then the activities in paragraph (1) are not subject to paragraph (2). Instead, all that paragraph (2) does is to indicate that processing to set up a database for, for example, medical research, is itself to be considered processing for medical research. To make processing under paragraph (1) subject to paragraph (2) it is necessary to read 'includes' as 'comprises'. The effect of this is that only activities of or for, for example, cancer registries for the purposes of paragraph (1) (e.g, medical research approved by a research ethics committee (REC)) are covered by paragraph (1) itself. However, while this fits the explanatory note, according to which 'Regulation 2 makes provision relating to the processing of patient information in connection with the construction and maintenance of databases by bodies (known as "cancer registries")', it needs to be noted that paragraph (1) appears to contrast 'comprise' with 'include', though it is not absolutely impossible that 'or' be read here as

indicating synonymy. Paragraph (4) also does not place conditions on paragraph (1) (which is what paragraph (1) being 'subject to' paragraph (4) suggests should be the case), as what it does is to empower the Secretary of State (when he or she considers processing for purposes under paragraph (1) to be 'necessary in the public interest') *to require* those who *may* process confidential patient information to process the confidential patient information (individuals and actions that are subject to conditions by paragraph (1) being 'subject to' paragraphs (2) and (3) and Regulation 7).

Regulation 5 permits confidential patient information to be processed for medical research *in the circumstances* set out in the Schedule to the Regulations, which are:

1. in the process of making this information less identifiable,
2. processing relating to present or past geographical locations required for research into the locations at which disease/other medical conditions may occur,
3. processing which enables the lawful holder to identify and contact patients to obtain consent in relation to research on them, their information, or their samples,
4. processing for medical purposes to link information, validate quality or avoid impairment of quality,
5. for audit, monitoring or analysis of the provision of patient care and services by health service, or
6. to grant access for one or more of these purposes,

*if* the processing is approved by both the Secretary of State and an REC, *subject to* Regulation 7 restrictions and exclusions, which are:

1. He or she shall not process that information more than necessary to achieve the purposes (Reg. 7.1).
2. As far as practical, remove any unneeded particulars (Reg. 7.1(a)), ensure no access is allowed to persons not involved in the processing (Reg. 7.1 (b)) and appropriate technical and organizational measures are taken to prevent unauthorized processing (Reg. 7.1 (c)).
3. Review at least every year the need to process such confidential patient information, and if it possible to reduce the amount processed (Reg. 7.1(d)).
4. No person shall process confidential patient information under these regulations unless he is a health professional (as defined by the DPA) or a person who owes a duty of confidentiality equivalent to that of a health professional (Reg. 7.2).

The Patient Information Advisory Group (PIAG) has been set up to advise the Secretary of State for the purposes of making regulations under Sections 60(1) and

(4)(b) of the Health and Social Care Act 2001.[25] However, the Health Service (Control of Patient Information) Regulations 2002 Regulation 2(5) requires that the PIAG scrutinize medical research subject to those Regulations. Both class and individual project approvals may be given under the regulations. There are two problems. First, given that the creation of the PIAG was authorized for one specific purpose in primary legislation, where is the authority for the creation of a secondary role for the PIAG created by other secondary legislation? Second, where approval is required by an REC, the REC must approve the project first before application may be made to PIAG. However, Regulation 5 does not indicate the order in which the application must proceed between the committees.

**Is there Lexical Ordering of Conditions for Legitimate Processing and of Processing of Sensitive Data?**

Nothing in the UK Act Schedules 7 (implementing Article 7) or Schedule 3 (implementing Article 8) explicitly states that consent of the data subject is necessary for legitimate processing or that explicit consent is necessary for the processing of sensitive personal data. Consent (Schedule 2) or explicit consent (Schedule 3) is simply listed as one of a number of conditions that can satisfy the relevant Schedule. However, because Section 3 of the Human Rights Act 1998 requires all UK legislation to be interpreted so as to be compatible with Articles 2–12 and 14 (as read through Articles 16–18) of the European Convention on Human Rights (ECHR) if it is possible to do so, it is arguable that consent must be obtained for the processing of sensitive personal data *unless* conditions that would satisfy a breach of Article 8(1) of the ECHR (as listed in Article 8(2) of the ECHR) are satisfied. (That is to say, the other conditions listed in Articles 7 and 8 may only be appealed to in circumstances in which a derogation under Article 8(2) ECHR applies). This is because Section 2(1) of the Human Rights Act 1998 requires the UK Courts to take account of the jurisprudence of the European Court of Human Rights. However, in, for example, *MS v Sweden,* it is clear that the European Court of Human Rights considers the processing of any data on a person's health without consent to engage Article 8(1) ECHR and require a justification in terms of Article 8(2) of the Convention. And while neither the UK Act nor the Directive explicitly states that consent must take lexical priority, neither instrument says anything that precludes such an interpretation, which renders an interpretation of lexical priority for consent possible in the terms of the Human Rights Act 1998.

The Commissioner is of the view that, whilst consent is not a prerequisite for processing of medical information under the 1998 Act *per se*, the Act nevertheless places a duty on data controllers to process data 'lawfully' (Sch.1, Part 1, para.1).

---

[25] The Secretary of State was given powers to establish the PIAG by the Health and Social Care Act section 61. This power was exercised in the Patient Information Advisory Group (Establishment) Regulations 2001, SI 2001 No. 2836, which came into force on 31 August 2001.

Consequently, health care information will be subject to requirements of common law confidentiality. There are three general exemptions to the duty of confidence: where there is a legal compulsion, an overriding public duty, or with consent.[26] Consent under common law requires three things; to be informed, the person giving it has choice, and an indication the individual has given his or her consent.[27]

## National Identification Number

Schedule 1 Part II paragraph 4 of the UK Act makes provision for the Secretary of State by order to specify when personal data may be fairly and lawfully processed using a 'general identifier', as required by Article 8(7) of the Directive. However, despite the fact that Article 8(7) states that 'Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed', no Order has been issued. This failure can surely only be legitimate if Article 8(7) may be interpreted as giving Member States discretion to specify that there are no conditions limiting the processing of personal data by use of a general identifier.

## Is there Removal of the Right to Object?

Section 10 of the UK Act (implementing Article 14(a) of the Directive) grants a right to prevent processing likely to cause substantial damage or distress. 'Substantial, unwarranted damage/distress' has been interpreted by the Commissioner as follows:

> It is for a court to decide in each case whether the damage or distress is substantial and unwarranted.
>
> The Commissioner takes the view that a data subject notice is, therefore, only likely to be appropriate where the particular processing has caused, or is likely to cause, someone to suffer loss or harm, or upset and anguish of a real nature, over and above annoyance level, and without justification.[28]

This right does not apply (s.10(2)) when processing is with the consent of the data subject, for the purposes of a contract of the data subject, necessary for a non-contractual legal obligation of the data controller, or in the vital interests of the data subject. It does apply where processing is to be rendered legitimate in the public interest or as necessary for the legitimate interests of the data controller, and no provision is made in the Act for removal of this right.

---

[26] Information Commissioner, *Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998* (Wilmslow: Information Commissioner, May 2002), 15–18.

[27] Ibid.

[28] Information Commissioner, *Data Protection Act 1998: Legal Guidance* (Version 1, Wilmslow: Information Commissioner, 1998), paragraph 4.2.1.

**Provision of Information to the Data Subject**

Articles 10 and 11 of the Directive are incorporated by Schedule 1 Part II paragraphs 2 and 3, which treats them as necessary conditions of fair processing under the 1st data protection principle duty to process data lawfully and fairly (cf. Article 6.1(a)).

All data controllers must provide the data subject with the following information:

a. the identity of the data controller,
b. if he has nominated a representative for the purposes of this Act, the identity of that representative,
c. the purpose or purposes for which the data are intended to be processed, and
d. 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 (Schedule 1 Part II paragraph 2(3).

Unlike Articles 10 and 11(1) of the Directive, no examples are provided. Furthermore, where data are obtained from the data subject (the 'Article 10 case'), the information must be provided only in so far as is practicable (Schedule 1 Part II paragraph 2.(1)(a)) (whereas Article 10 contains no reference to a qualification on the basis of practicability).

In any other case (the 'Article 11 case'), the information must be provided so far as practicable, which provides for a derogation where the provision would be impossible (Schedule 1 Part II paragraph 2(1)(b)), unless doing so would involve disproportionate effort (Schedule 1 Part II paragraph 3(1) and 3(2)(a)) or the data controller is under a non-contractual legal obligation to record the information contained in the data or to disclose the data (Schedule 1 Part II paragraph 3(1) and 3(2)(b)) or the Secretary of State so prescribes by order (Schedule 1 Part II paragraph 3(1)). Apart from the fact that Article 11(2) refers to impossibility rather than impracticability, this appears to be in line with Article 11(2). In addition, where the provision of information would involve disproportionate effort, Articles 4 and 5 of the Data Protection (Conditions under Paragraph 3 of Part II of Schedule 1) Order 2000 (SI 2000 No. 185) must also be satisfied if there is to be exemption from the requirement to provide the information (Article 3(1) of SI 2000 No. 185). Article 4 of SI 2000 No. 185 must also be met if there is to be exemption on the grounds of a non-contractual legal obligation of the data controller (other than an obligation conferred under any enactment or imposed by order of a Court) (Article 3(2)). Where it is decided that information is not to be made available to the data subject when the information has come to the data controller not directly from the data subject in an exempt situation indicated above, the information may only be denied if Article 4(2) conditions are met, namely that:

a. no notice in writing[29] has been received at any time by the data controller from an individual, requiring that data controller to provide the information set out in paragraph 2(3) of [Part II of Schedule 1 of the 1998 Act] before the relevant time (as defined in paragraph 2(2) of that Part) or as soon as practicable after that time; or

b. where such notice in writing has been received but the data controller does not have sufficient information about the individual in order readily to determine whether he is processing personal data about that individual, the data controller shall send to the individual a written notice stating that he cannot provide the information set out in paragraph 2(3) of that Part because of his inability to make that determination, and explaining the reasons for that inability.

Article 5(2) conditions must also be met:

> the data controller shall record the reasons for his view that the primary condition referred to in [paragraph 3(2)(a) of Schedule 1 Part II of the 1998 Act[30]] is met in respect of the data.

**Simplification to Notification**

If the data which form the basis for the medical research are 'non-automated accessible records' then there need be no notification to the Commissioner. There is also an exemption under Schedule 8, Part IV, paras. 15–17 up to the 24 October 1998, but only in relation to historical research, not medical research. Otherwise, there are no special provisions for notification regarding medical research (unless the data are anonymized, in which case the data are no longer personal data).

**Prior Checking**

Section 22(2) requires the Information Commissioner to subject 'assessable processing', which is processing that (see s.22(1)) is specified by order of the Secretary of State to be particularly likely 'to cause substantial harm or substantial distress to data subjects' or 'otherwise significantly to prejudice the rights and freedoms of data subjects' to prior checks. However, no such orders have, as yet, been issued.

Specific provision has been made in s.60 of the Health and Social Care Act 2001 for the processing of patient information for medical purposes. The reader should note that Regulation 2(5) of the Health Service (Control of Patient Information) Regulations 2002 makes it a requirement for processing confidential

---

[29] Article 4(3) indicates that 'in writing' means '(a) transmitted by electronic means, (b) is received in legible form, and (c) is capable of being used for subsequent reference'.

[30] That the notification would require a disproportionate effort or that the processing is necessary for a non-contractual legal obligation upon the data controller.

medical information to inform the PIAG and (ultimately) the Secretary of State of the processing.

## Publicizing of Processing Operations

In relation to Article 21, Section 19(6) requires the Information Commissioner to make publicly available all information in the register of notifications (see ss.17–19) kept by the Commissioner. Section 24 requires data controllers to make the 'registrable particulars' (see s.16(1)(a)–(f)) available in writing to any person who makes a written request for them in cases where notification is not required by Section 17(1) by virtue of Section 17(2)–(3) or notification per Section 18 has not been made.

## Standing to Bring Breaches to the Attention of the Supervisory Authority

According to Section 42(1)

> A request may be made to the Commissioner by or on behalf of any person who is, or believes himself to be, directly affected by any processing of personal data for an assessment as to whether it is likely or unlikely that the processing has been carried out in compliance with the provisions of this Act.

A data subject has a right to be informed by a data controller of the processing of personal data relating to him (or her) (Section 7), and rights to serve notices on a data controller requiring the data controller to:

i. cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject on the ground of substantial damage or distress being caused or likely to be cause to 'him or to another' (s.10(1));
ii. cease or not begin processing of data in respect of which he is the data subject for purposes of direct marketing (s.11);
iii. ensure that no decision that significantly affects the data subject is based solely on processing by automatic means (s.12).

If the data controller fails to comply with any one of these requests or notices then the data subject may apply to the High Court or a county Court (or, in Scotland, the Court of Session or the sheriff (s.7(9); s.10(4); s.11(2); s.12(8); s.15)).

An individual who suffers damage by reason of any contravention of the Act may bring an action for damages in these Courts (s. 13, s.15).

The Act does not provide for third parties to bring contraventions to the notice of the Commissioner or to take action in the Courts. This means that RECs do not have standing under the Act to bring proceedings *per se*, save perhaps in the

context of 'enforcement notices' where the source of a complaint appears irrelevant.

## Adequate Safeguards and the Optional Derogation from Article 25 on Third Country Transfers using Article 26.2

The 8th data protection principle (Schedule 1 Part I paragraph 8) provides that personal data may not be transferred to a third country that does not provide for an *adequate* level of protection. One of the exemptions to this rule is that the transfer is made on terms (Schedule 4 paragraph 8) or is made in such a manner (Schedule 4 paragraph 9) that the Information Commissioner approves or authorizes as ensuring adequate safeguards. The Information Commissioner must inform the European Commission and other EEA States of approvals granted for the purposes of Schedule 4 paragraph 8 and authorizations granted for the purposes of Schedule 4 paragraph 9 (s.54(7)) (cf. Article 26(3)).

In Directive Article 26.2, it states a member state may authorize a transfer to a third country (without an adequate level of protection) 'where the controller adduces adequate safeguards... [which] may in particular result from appropriate contractual clauses.' The EU (Article 26.4) may also decide that certain contractual clauses offer the sufficient safeguards required in Article 26.2, which member states shall take the necessary measures to comply with. The Commission decision 2001/497/EC of June 2001 decided on such standard contractual clauses 'with respect to the protection of privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights (Article 26.2)' and are therefore seen to provide adequate safeguards. These so-called 'model contract terms' have been approved by the UK IC.

The UK IC states that in relation to adequate safeguards for transfers:

> it can be seen that whether there is adequacy can, at least partly, be in the hands of the UK data controller. The data controller might limit the types of data transferred, the types of organisation they are transferred to or insist, whether through a contract or otherwise, on the recipient meeting certain conditions.[31]

The Information Commissioner states that there are several different types of contract that can be used to ensure adequate protection. These are: those based on standard terms agreed by either the EC (most common) or those agreed solely by the Information Commissioner (rare), contracts drawn-up by the data controller, or one-off arrangements authorized by the IC (also rare). Contracts drawn-up by the data controller will not be checked by the IC unless in exceptional circumstances, they can be used to 'plug the gaps' of adequacy or when the controller is in no position (or does not want) to judge adequacy themselves.

---

[31] Information Commissioner, *International Transfers of Personal Data: Advice on Compliance*, 2001, 7.5.

Where the European Commission makes a decision under Article 31(2) for the purposes of Article 26(3) or (4), the Information Commissioner must disseminate this decision (s.51(6)(b)) (cf. Article 26(3) & (4)) and comply with it (s.54(6)). In comparison, the European Commission may make a decision under Article 25(6) that a third country provides adequate protection for the fundamental rights and freedoms covered by the Directive. In such a case there is no specific provision in the UK legislation to act on the decision, though such a decision of the EC may be relevant information for dissemination to data controllers by the Information Commissioner under the general duty in Section 51(6)(c) of the 1998 Act.

**The Supervisory Authority**

Medical research and the use of medical data is not treated as a special sector with its own supervisory authority. The use of personal data for medical research is dealt with directly by the Information Commissioner. The powers given to the supervisory authority include those outlined below:

- To receive requests by or on behalf of any person who is, or believes himself to be, directly affected by any processing of personal data for an assessment as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of this Act (s. 42.1).
- Can issue 'information notices' (s.43) or 'special information notices' (s. 44), which require information to be provided to the Commissioner to aid the assessment of a request.
- Can issue 'enforcement notices' (s. 40), when the Commissioner is satisfied the data controller has contravened or is contravening any of the data protection principles. This notice can order the controller to refrain from processing (s 40.1(b)), to rectify, block, erase or destroy data (s 40.3), or to inform third parties to whom the information has been disclosed of this (s 40.5).
- A judge can issue a warrant so the Commissioner can search premises, to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal data (Schedule 9). The Information Commissioner can also seize data.
- In some cases, it authorizes processing (Section 53), and Court proceedings should be enacted by the Commissioner (Article 60).

**Penalties for Infringement**

Apart from direct recourse to a Court on the application of the data subject (see section above on standing to bring breaches to the attention of the supervisory authority), the Act provides for the following measures to ensure implementation of the provisions of the Directive.

The Information Commissioner may:

- issue enforcement notices for contravention of any of the data protection principles (s.40)
- act on requests for assessment (s.42)
- serve information notices (s.43)
- serve special information notices (in relation to the 'special purposes' of journalism, literature and art of Section 32)

and the Information Commissioner has powers of entry and inspection (s.50 & Schedule 9).

It is an offence under the Act:

- to process personal data without notifying the Information Commissioner as required by Section 17(1) (s.21(1)) or to contravene the notification regulations (see the Data Protection (Notification and Notification Fees) Regulations 2000, SI No. 188) made under Section 20(1) (s.21(2)),
- to carry out assessable processing in contravention of Section 22(5) (s.22(6)) (however, no regulations (per s.22(1)) to identify assessable processing have yet been made),
- not to provide the information specified in Section 16(1) within 21 days to any person who requests this in writing when Section 24(1) applies (s.24(4)),
- not to comply with an enforcement, information or special information notice (s.47) (however, these notices may be appealed against to the Information Tribunal [concerning which, see Schedule 5 Part II, Schedule 6, the Data Protection Tribunal (Enforcement Appeals) Rules 2000, SI No. 189, the Data Protection Tribunal (National Security Appeals) Rules 2000, SI No. 206, the Data Protection Tribunal (National Security Appeals) (Telecommunications) Rules 2000] (s.48 & s.49(1)–(5)) and from there to a Court (s.49(6))),
- to obtain or disclose (or procure the disclosure to another of) personal data or information contained in personal data without the consent of the data controller (s.55(1) & (3)),
- to sell personal data obtained in contravention of Section 55(1) (s.55(4)),
- to offer to sell personal data (which includes to advertise that personal data are or may be for sale—Section 55(6)) obtained or subsequently obtained in contravention of Section 55(1) (s.55(5) unless Section 28 applies (s.55(8)). (For the purposes of s.55(4)–(6), personal data includes not only information 'contained in' personal data per Section 1(2), but information 'extracted from' personal data (s.55(7))),
- to require certain records to be produced (or to produce certain records) as specified by Section 56(1) or (2) (s.56(5)),
- to obstruct (or fail to assist) persons executing a warrant granting the power to enter and inspect as provided by Section 50 (Schedule 9 paragraph 12).

Prosecution for offences requires the consent of the Information Commissioner or the Director of Public Prosecutions (England and Wales) or the Director of Public Prosecutions of Northern Ireland (Northern Ireland (s.60(1)). In Scotland, prosecutions can only be brought by the Crown Office and the Procurator Fiscal

Service. A Procurator Fiscal can prosecute either acting on a report from the police or Information Commissioner or independently.[32]

The penalties for offences are listed in Section 60(2)–(4). Fines may be levied (s.60(2) and (3)) and the Courts may order documents to be forfeited, destroyed or erased for various offences (s.60(4)). Except for the offence of failing to assist or obstructing a person with a warrant under the Act, a person guilty of any offence under the Act is liable on summary conviction to a fine not exceeding the statutory maximum (£5000) or, on conviction or indictment to an unlimited fine (s.60(2)). For offences relating to the carrying-out of a warrant, the penalty on summary conviction is not to exceed level 5 on the standard scale (£5000) (s.60(3)).

Officers of corporate bodies may be held liable for offences committed by these bodies (s.61).

While a breach of, e.g., the common law on confidentiality (or any of the UK's other laws on lawful processing of personal data) is a breach of the 1st data protection principle (Schedule 1 Part I paragraph 1), it does not as such constitute an offence under the Act. However, as a breach of a data protection principle it may lead to the serving of an enforcement notice (see s.40(1)). If this is not complied with, this constitutes an offence (s.47(1)).

**Exemption from Liability**

As permitted by Article 23(2); Section 13(3), provides that it is a defence in an action for damage caused by processing of personal data for a data controller to prove that 'he had taken such care as in all the circumstances was reasonably required to comply' with a requirement of the Act. In addition, it is a defence for a person charged with an offence in relation to failure to comply with the duty imposed by notification regulations made under Section 20(1) or and the duty to notify of section 24(1) 'to show that he exercised all due diligence to comply with the duty' (s.21(3); s24(5)). The following offences are strict liability offences:

- Processing without notification (S.21(1));
- Processing before expiry of assessable processing time limits or assessable processing notice from Commissioner (s.22(6));
- Enforced Subject Access (s.56(5))—this offence concerns supply of 'relevant records' where a statutory exception does not apply.

**Definition of Explicit Consent**

The Act contains no definition or clarification of 'explicit consent'. However, the Information Commissioner's guidance to the Act states that in relation to consent, there must be some active communication between the parties, which may be other

---

[32] We are grateful to Lindsey Anderson, Principal Depute in the Crown Office Policy Group for indicating the position in Scotland.

than writing.[33] It states that the explicit consent needed for processing sensitive data, means that the consent must be 'absolutely clear' and should cover (in appropriate cases) the specific detail of the processing, the type of data, purposes and any specific aspects of the processing which may affect the individual (for example, disclosures).[34]

## Transitional Exemptions

With reference to Article 32, Schedule 8 grants a complex set of transitional exemptions. Generally, the Act applied fully (subject to permanent exemptions & special exceptions) to

- automated & manual processing begun after 23 Oct 1998 immediately the Act came into force;
- automated processing begun before 24 Oct 1998 only from 24 Oct 2001; and
- manual processing begun before 24 Oct 1998 only from 24 Oct 2007.

Until 24 Oct 2001, 'eligible manual data' (i.e., manual data subject to processing already underway before 24 Oct 1998) (except for data relevant to the financial standing of the data subject in respect of which the data controller is a credit reference agency) was exempt from data protection principles and Parts II and III of the Act (Schedule 8 paragraph 2(1)), unless the data were held in an accessible record (which includes a health record), in which case Sections 7 & 15 (in part) and 12A apply (Schedule 8 paragraph 3(1)(a) & (2)), which also apply to 'non-eligible' manual records not in a relevant filing system (Schedule 8 paragraph 3(1)(b) and (2)). Contrary to what is suggested by Department of Health guidance,[35] there is no transitional exemption for 'non-eligible' manual health records in a relevant filing system.

From 24 Oct 2001–24 Oct 2007, eligible manual data held immediately before 24 October 1998, together with non-eligible manual data that are not intended to be processed automatically or that do not form part of a relevant filing system but nevertheless form part of an accessible record, are exempt from the 1st data protection principle *except for* the fair processing code (Schedule 1 Part 2 paragraph 2) implementing Articles 10 and 11, the 2nd, 3rd, 4th, and 5th data protection principles, and Sections 14(1)–(3)) (implementing the right to rectification, blocking, erasure and destruction).

---

[33] Information Commissioner, *Data Protection Act 1998: Legal Guidance* (Version 1, Wilmslow: Information Commissioner, 1998) paragraph 3.1.5.

[34] Ibid.

[35] The Guidance is found in Health Service Circular HSC 2000/009 'Data Protection Act 1998: protection and use of patient information' and is supported by information on the Department of Health website of the same name at http://www.doh.gov.uk/dpa98/index.htm (last accessed on 16th September 2003). The guidance on transitional provisions is at Part 2 of the information.

Eligible automated data were exempt from the Act until 24 Oct 2001 *if* they were not processed with reference to the data subject (Schedule 8 paragraph 5). Otherwise, this data were exempt until 24 Oct 2001 from the fair processing code of the 1st data protection principle; the 7th data protection principle (as far as it requires compliance with Schedule 1 Part II paragraph 12); the 8th data protection principle; Section 7(1)(b), (c)(ii) & (d); Sections 10–12; and Section 13 (except in 4 specific circumstances) (Schedule 8 paragraph 13).

The Act applied fully immediately to non-eligible automated data.

**Exemption for Historical Research**

Insofar as manual personal data were subject to processing already under way 'immediately before 24th October 1998', it is exempt from the first data protection principle *except* the fair processing provisions of Schedule 1 Part II paragraph 2, the 2nd–5th data protection principles and Section 14(1)–(3), *provided that* the relevant conditions (see s.33.(1)(a)) are met *and* the data are processed only for historical research (Schedule 8 Part I, paragraphs 1(1) and (2) and Part IV, paragraphs 15–16).

Insofar as automated personal data were subject to processing already under way immediately before 24 October 1998, it is exempt from the first data protection principle *except* the fair processing provisions, *provided that* the relevant conditions are met *and* the data are processed only for historical research (Schedule 8 Part I, paragraph 1(1) & 2, and Schedule 8 Part IV paragraphs 15 and 17(1)). The same data are additionally exempt from the 2nd–5th data protection principles and Section 14(1)–(3), *provided that* it is also the case that the data are not processed by reference to any data subject (Schedule 8 Part I, paragraphs 1(1) and (2), and Schedule 8 Part IV paragraphs 15 & 17(2)).

Disclosing data (a) 'to any person, for the purpose of historical research only', or (b) 'to the data subject or a person acting on his behalf', or (c) 'at the request, or with the consent, of the data subject or a person acting on his behalf', or where the person disclosing has reasonable grounds for believing that (a), (b), or (c) applies, is not, *by itself*, to be treated as processing for a purpose other than historical research, and so is covered by the exemptions (Schedule 8 Part IV, paragraph 18)).

Since Article 32(3) of the Directive permits Member States to exempt processing for the sole purpose of historical research from the whole of the first data protection principle, and the provisions of Schedule 1 Part II paragraph 2 (which are intended to implement Articles 10 & 11) are essentially conditions of fair processing under the first principle, in this respect, the Act (by not extending the exemption to the first data protection principle to the provisions of Schedule 1 Part II paragraph 2) provides a narrower exemption than the Directive permits.

However, what constitutes 'historical research' is not defined. It must, however, be distinguished from research for historical purposes, to which the general less extensive exemption for research, history and statistics of Section 33 applies.

## Are DNA Samples Treated as Personal Data?

The official view from the IC is that samples themselves are not treated as personal data, because it is physical material. As 'processing' personal data includes obtaining the data, the analysis of genetic material that reveals information about a particular individual comes within the scope of the Act. The Medical Research Council's current view is that data extrapolated from tissue samples are to certainly to be regarded as 'personal data', as well as any identifiers used in connection with an archive sample.[36] However, the MRC's view does not appear to be that the tissue sample itself ought to be regarded as personal data. The Human Genetics Commission is of a similar opinion.[37] This makes sense, as the definitions of 'data' under s.1(1) clearly do not envisage physical tissue samples as coming within the definition (after all, it is not automated data, nor 'information'—and it would be difficult to say that it is a 'relevant filing system' as the sample itself is not a 'set of information'). It may be possible to say that it is a 'health record' within the meaning of s.68(2)(b) ('..."health record" means any record which ... has been made by or on behalf of a health professional in connection with the care of that individual'). However, this is stretching the definition quite some way, and s.1(1) still requires an 'accessible record' to consist of information anyway. In any event, if the tissue sample has not been taken and included with the health record in connection with the care of the data subject, it will not fall within this definition.

Consequently, it is possible to conclude that tissue samples are not 'personal data' under the Act. However, in most respects, this is academic. After all, the term 'processing' includes 'obtaining, recording or holding the information or data'. Applied to tissue samples, this means that any attempt to derive identifiable information from a sample with respect to a living person will engage the 1998 Act. Furthermore, even if the derived information is anonymized, then it may still be possible to identify the data subject either through markers on the sample archive, or due to an unusual genetic profile/mutation which either (a) manifests itself physically, or (b) may be identified inadvertently through further screening of the data subject.

---

[36] Medical Research Council Ethics Series, *Human Tissue and Biological Samples for Use in Research* (London: Medical Research Council, 2001), paragraph 5.1.
[37] Human Genetics Commission, *Inside Information: Balancing interests in the use of personal genetic data* (London: Human Genetics Commission, May 2002), paragraph 3.43.